

Vertrag über die Verarbeitung von Daten im Auftrag für Q.wiki Now!

Version 2.26 - Aktiv ab 01.10.2026

Präambel

Der Auftraggeber („Verantwortlicher“) möchte den Auftragnehmer („Auftragsverarbeiter“) mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

§ 1 Begriffsbestimmungen

Für in dieser Vereinbarung benutzte Begriffe, die in Art. 4, 9 und 10 DS-GVO definiert werden, gilt diese gesetzliche Definition in der im Zeitpunkt des Vertragsschlusses geltenden Fassung auch für diesen Vertrag.

§ 2 Vertragsgegenstand

2.1 Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Software as a Service auf Grundlage des Hauptvertrags. Dabei erhalten der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte Zugriff auf personenbezogene Daten und verarbeiten diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und, sofern vorhanden, aus der dazugehörigen Leistungsbeschreibung) sowie aus der Anlage 1 zu diesem Vertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

2.2 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrags vor.

2.3 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht über die Laufzeit des Hauptvertrages hinausgehende Verpflichtungen ergeben. Sich aus diesem Vertrag ergebende Kündigungsrechte bleiben von der vorstehenden Regelung unberührt.

2.4 Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

2.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Weisungsrecht

3.1 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm dies rechtlich gestattet ist.

3.2 Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher, in Textform oder über die zur Verfügung gestellte Software durch

einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung und Löschung von Daten sowie auf die Einschränkung der Verarbeitung.

3.3 Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

3.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten der ebenfalls in Anlage 1 näher spezifizierten betroffenen Personen. Diese Daten können die in Anlage 1 aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten umfassen, sofern vom Auftraggeber eingebracht.

§ 5 Technische und organisatorische Maßnahmen des Auftragnehmers

5.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht ohne entsprechende Weisung an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen in Papierform und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen getroffen hat. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung welche Maßnahmen getroffen werden und die Umsetzung der Maßnahmen offen. Eine Verbesserung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten und der Auftraggeber über wesentliche Veränderungen unverzüglich informiert wird.

5.3 Ansprechpartner für den Datenschutz, beim Auftragnehmer ist:

Ariadne GmbH, Am Kraftversorgungsturm 5, 52070 Aachen, Deutschland, zu Händen:
Datenschutzbeauftragter, datenschutz@ariadne.io

Ein Wechsel in der Person des Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

5.4 Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b DS-GVO), über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren und mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen der Mitarbeiter auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

6.1 Bei Störungen bei den Verarbeitungstätigkeiten, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers oder Verdacht auf sonstige sicherheitsrelevante Vorfälle beim Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, in Textform informieren. Die Erstmeldung kann vorläufig sein, fehlende oder neue Informationen werden ohne unangemessene Verzögerung nachgereicht. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, die für den Auftraggeber relevante Verarbeitungen oder Sachverhalte betreffen. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

6.2 Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffene(n) Person(en), informiert hierüber den Auftraggeber, ersucht ihn um weitere Weisungen und erteilt dem Auftraggeber jederzeit weitere Auskünfte, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

6.3 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

6.4 Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

6.5 An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Datenschutz-Aufsichtsbehörden gem. Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers, sofern möglich, nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Vor-Ort-Prüfungen erfolgen nachrangig, d. h. nur, wenn die zuvor bereitgestellten Auskünfte, Testate, Zertifizierungen oder Fragebögen für eine angemessene Beurteilung nicht ausreichen.

7.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen,

die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Anlage 2 erforderlich sind.

Unterstützungsleistungen, die darüber hinausgehen, sind vom Auftraggeber zu erstatten. Dies gilt nicht für Unterstützungsleistungen, die aufgrund einer behördlichen Anordnung, eines Sicherheitsvorfalls bei dem Auftragnehmer oder eines wesentlichen Verstoßes des Auftragnehmers gegen diese Vereinbarung erforderlich werden.

Vor-Ort-Prüfungen sind mit einer Frist von mindestens 14 Kalendertagen in Textform anzukündigen und finden höchstens einmal innerhalb von zwölf Monaten statt. Sie sind auf einen Prüfungstag in der Zeit von 9:00 bis 18:00 Uhr zu begrenzen; reicht dieser nachweislich nicht aus, kann die Prüfung im gegenseitigen Einvernehmen auf unmittelbar anschließende Werktage ausgedehnt werden. Führt der Auftraggeber eine darüberhinausgehende Prüfung durch, ohne dass der Auftragnehmer hierzu Anlass gegeben hat, hat der Auftragnehmer Anspruch auf Erstattung der ihm hierdurch entstehenden angemessenen Kosten.

Reise- und Übernachtungskosten sowie ein angemessener Tagessatz des Auftragnehmers werden vom Auftraggeber getragen.

7.3 Der Auftraggeber dokumentiert das Ergebnis der von ihm durchgeführten Kontrollen und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7.4 Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 5 Abs. 4 auf Verlangen nach.

§ 8 Einsatz von Subunternehmern

8.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung weitere Unterauftragnehmer i.S.d. Art. 28 DSGVO zur Erfüllung seiner vertraglich vereinbarten Leistungen in Anspruch zu nehmen. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 3 zu diesem Vertrag angeben. Der Auftraggeber ist über jede beabsichtigte Hinzuziehung oder Ersetzung von Unterauftragnehmern im Vorfeld zu informieren.

8.2 Der Auftraggeber kann gegen die Begründung weiterer oder die Ersetzung von Unterauftragsverhältnissen binnen einer Frist von 2 (zwei) Wochen nach Zugang der Information über die Änderung schriftlich oder in Textform Einspruch erheben. Im Falle des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung des Auftragnehmers nicht möglich ist – die von der Änderung betroffenen Leistungen gegenüber dem Auftraggeber aus wichtigem Grund kündigen.

8.3 Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (zB durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

Sollte die Angemessenheit des Schutzniveaus nach dem EU-U.S. Data Privacy Framework (Art. 45 DSGVO) entfallen, stellt der Auftragnehmer unverzüglich sicher, dass die betroffenen Datenübermittlungen auf Grundlage der EU-Standarddatenschutzklauseln (SCC) sowie eines ergänzenden Transfer Impact Assessments (TIA) fortgeführt werden, und informiert den Auftraggeber hierüber.

8.4 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören zB Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse iSv Abs. 1 dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

9.1 Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12 – 22 sowie 32 und 36 DSGVO.

9.2 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

10.1 Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

10.2 Der Auftragnehmer stellt den Auftraggeber von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DS-GVO auferlegten Pflicht oder wegen der Nichtbeachtung oder Verletzung einer in dieser Vereinbarung festgelegten Pflicht oder einer vom Auftraggeber gesondert erteilten Weisung geltend machen.

10.3 Die Parteien stellen sich jeweils von der Haftung frei, wenn/soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DS-GVO.

10.4 Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 12 Beendigung des Hauptvertrags

12.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen in Papierform, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Herausgabe- bzw. Vernichtungsverpflichtung betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen.

12.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten

prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Etwaige für die Beauftragung und die Prüfung durch einen Dritten anfallende Kosten trägt der Auftraggeber.

12.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Informationen vertraulich zu behandeln.

§ 13 Kirchlicher Datenschutz

13.1 Für einen Auftraggeber, der dem Gesetz über den Kirchlichen Datenschutz (KDG) unterliegt, beziehen die Parteien die §§ 29 – 33 KDG sowie die Beachtung der dort getroffenen Vorschriften zur Auftragsverarbeitung ausdrücklich ein.

13.2 Für einen Auftraggeber, der dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) unterliegt, beziehen die Parteien die §§ 30 – 32 DSG-EKD sowie die Beachtung der dort getroffenen Vorschriften zur Auftragsverarbeitung ausdrücklich ein.

§ 14 Schlussbestimmungen

14.1 Die Parteien sind sich darüber einig, dass dem Auftragnehmer kein Zurückbehaltungsrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger zusteht.

14.2 Änderungen und Ergänzungen dieses Vertrags, die Erklärung einer Kündigung sowie die Abänderung dieser Klausel bedürfen zu ihrer Wirksamkeit der Textform.

14.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

14.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Aachen.

§ 15 Anlagen

Folgende Anlagen sind Bestandteil dieser Vereinbarung zur Auftragsverarbeitung:

- Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien
- Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers
- Anlage 3 – Genehmigte Subunternehmer

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Art(en) der personenbezogenen Daten:

Als Art der personenbezogenen Daten die im Auftrag verarbeitet werden kommen sämtliche Daten in Betracht, die der Auftraggeber freiwillig im Rahmen der interaktiven Managementsystemsoftware Q.wiki verarbeitet. Dabei handelt es sich üblicherweise insbesondere um

- Kundenstammdaten (z.B. Name, Anschrift, Ansprechpartner, Kontaktdaten)
- Kommunikationsdaten
- Nutzungs- und Inhaltsdaten sowie
- unternehmensbezogene Daten (Rolle, Standort, Abteilung)

Der Auftragnehmer erhebt oder verarbeitet im Rahmen des Betriebs von Q.wiki grundsätzlich keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO. Eine Verarbeitung derartiger Daten findet nur statt, wenn der Auftraggeber solche Informationen eigenverantwortlich und freiwillig in das System einbringt. In diesen Fällen erfolgt die Verarbeitung ausschließlich im Rahmen der Weisungen des Auftraggebers und auf Grundlage dieser Vereinbarung zur Auftragsverarbeitung.

Kategorien betroffener Personen:

Der Kreis der von der Datenverarbeitung betroffenen Personen ist abhängig von dem Personenkreis, dem der Auftraggeber den Zugang zur interaktiven Managementsystemsoftware Q.wiki eröffnet. Dabei kann es sich insbesondere um

- Mitarbeiter und Kunden des Auftraggebers sowie
- um weitere Dritte handeln (z.B. technische Dienstleister/Interessenten oder Berufsgeheimnisträger wie Steuerberater oder Rechtsanwälte).

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Zertifizierung: Der Auftragnehmer betreibt ein Informationssicherheits-Managementsystem (ISMS) und ist nach ISO/IEC 27001 zertifiziert. Ein aktuelles Zertifikat kann auf Anfrage bereitgestellt werden.

Providerstandards: Physische Sicherheit und Rechenzentrumsbetrieb erfolgen nach anerkannten Standards des Cloud-/RZ-Anbieters (z. B. ISO/IEC 27001).

Vertraulichkeit

Zutrittskontrolle (physischer Zugang)

- Zugang über vom Vermieter betriebenes Chipkarten-/Transponder-System,
- Schlüssel-/Transponderverwaltung durch den Vermieter
- Besuchermanagement mit Anmeldung und Begleitung,
- Einsatz externer Reinigungs- und Wachdienste nur nach sorgfältiger Auswahl und Vertraulichkeitsverpflichtung.

Zugangskontrolle (logischer Systemzugang)

- Starke Authentisierung: Nutzung separater Administrationskonten.
- Passwortrichtlinie: Mindestlänge 12 Zeichen, sichere Speicherung nach Stand der Technik.
- Unterstützung von Single Sign-On
- Administrationszugänge: IP-Restriktionen für administrative Zugriffe werden eingesetzt, soweit technisch möglich und vereinbart.

Zugriffskontrolle (Berechtigungen und Datenzugriff)

- Rollen- und Berechtigungskonzept nach dem Least-Privilege-Prinzip, Rechteverwaltung durch autorisierte Mitarbeitende (Operations/Administration).
- Trennung von Arbeits- und Administrationskonten, Anzahl privilegierter Konten auf das notwendige Minimum reduziert.
- Joiner/Mover/Leaver: Zügige Einrichtung/Änderung/Entzug von Berechtigungen bei Personalwechseln.
- Datenträger/Medien: Logische Löschung vor Wiederverwendung, physische Vernichtung interner Datenträger nach ISO/IEC 21964, sofern angefallen. Für Cloudspeicher gelten die zertifizierten Verfahren des Anbieters.

Mobiles Arbeiten

- Verwaltete, verschlüsselte Endgeräte: Mobile Arbeit erfolgt ausschließlich über vom Auftragnehmer verwaltete, vollverschlüsselte Endgeräte unter MDM-Steuerung; Geräte können bei Bedarf aus der Ferne gesperrt bzw. gelöscht werden.
- Zugriffsschutz: Remote-Zugriffe auf Systeme/Daten erfolgen nur über dem Stand der Technik entsprechende, verschlüsselte Verbindungen und mit Mehrfaktor-Authentisierung.
- Rechte- und Gerätesicherheit: Rollen- und bedarfsorientierte Rechtevergabe (Least Privilege), keine lokalen Adminrechte für Standardnutzer. MDM-Compliance erzwingt aktuelle Sicherheitsupdates sowie Bildschirmsperre/Timeout.
- Datensparsamkeit: Arbeitsdaten werden vorrangig in zentralen, kontrollierten Diensten verarbeitet, lokale Speicherung auf Endgeräten wird auf das notwendige Minimum beschränkt. Nutzung ausschließlich freigegebener Anwendungen/Dienste.

- Vorfallsbehandlung: Verlust/Diebstahl mobiler Endgeräte ist unverzüglich zu melden, es erfolgen umgehend Remote-Sperre/-Löschung und eine Bewertung möglicher Risiken. Erforderliche Meldungen nach DSGVO werden vom Auftragnehmer in Abstimmung mit dem Auftraggeber vorgenommen.
- Schulungen: Alle Mitarbeitenden erhalten mindestens jährlich verpflichtende Schulungen, einschließlich spezifischer Anforderungen an mobiles Arbeiten.

Pseudonymisierung und Verschlüsselung

- Datenübertragung: Alle Verbindungen zum Q.wiki erfolgen verschlüsselt
- Datenspeicherung (at rest): Verschlüsselung ruhender Daten durch aktuelle, vom BSI als sicher anerkannte Verschlüsselungsverfahren.
- Pseudonymisierung systembedingt nicht erforderlich

Trennungskontrolle (Trennungsgebot)

- Mandantentrennung: Technische Trennung der Kundendaten durch Mandantenlogik, Zugriffsprüfungen auf Mandantenebene.
- Umgebungen: Strikte Trennung von Entwicklungs-, Test- und Produktivsystemen

Integrität

Eingabekontrolle

- Verarbeitung personenbezogener Daten ausschließlich unter individuellen Benutzerkonten, Gruppenkonten werden vermieden.
- Verfahren und Verantwortlichkeiten für freigabepflichtige Änderungen sind definiert

Weitergabe-/Übertragungskontrolle

- Übermittlungen personenbezogener Daten zwischen Systemkomponenten, Standorten und gegenüber berechtigten Dritten erfolgen ausschließlich über verschlüsselte Verbindungen.
- Internationale Übermittlungen: Datenübermittlungen in Drittländer außerhalb des EU/EWR erfolgen ausschließlich an die in Anlage 3 aufgeführten Unterauftragnehmer auf Basis des EU-U.S. Data Privacy Framework (Art. 45 DSGVO) oder einer anderen zulässigen Rechtsgrundlage gem. Art. 44 ff. DSGVO nach vorheriger Information.

Verfügbarkeit und Belastbarkeit

- Betrieb auf hochverfügbarer Cloud-Infrastruktur
- Reduzierung von Ausfallrisiken durch redundante Komponenten und den Betrieb in professionellen Rechenzentrumsumgebungen des Cloud-Anbieters
- Kapazitätsmanagement und geregelte Betriebsprozesse zur Aufrechterhaltung der Servicequalität
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz- und Informationssicherheitsmanagement

- Unternehmensweite Leitlinien zu Datenschutz und Informationssicherheit, Vertraulichkeitsverpflichtung aller Mitarbeitenden und regelmäßige Schulungen
- Betrieb eines zertifizierten ISMS nach ISO/IEC 27001, kontinuierliche Verbesserung der Sicherheitsmaßnahmen
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO (z. B. rollenbasierte Rechte mit minimalen Standardberechtigungen)

Umgang mit Sicherheitsvorfällen

- Verfahren zur Identifikation, Eindämmung, Beseitigung und Nachbereitung von Sicherheitsvorfällen

- Unterstützung des Auftraggebers bei der Erfüllung seiner Pflichten nach Art. 33/34 DSGVO (Meldung/Benachrichtigung), einschließlich Bereitstellung verfügbarer Informationen zum Vorfall
- Löschung und Rückgabe von Daten
- Nach Vertragsende erfolgt die Verarbeitung nur noch zum Zweck der geordneten Beendigung

Endgerätesicherheit (Mitarbeitende)

- Unternehmensgeräte mit Festplattenverschlüsselung, aktuellen Sicherheitsupdates und personalisierten Benutzerkonten
- Sichere Remote-Arbeit (z. B. VPN) und Baseline-Härtung der Endgeräte, Richtlinien zum Umgang mit Wechseldatenträgern

Auftragskontrolle und Subprozessoren

- Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers, interne Richtlinien verhindern unbefugte Verarbeitung
- Vertraulichkeitsverpflichtung aller Personen mit Zugang zu personenbezogenen Daten

Anlage 3 – Genehmigte Subunternehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten ("Unterauftragnehmer"). Dabei handelt es sich um nachfolgende Unternehmen:

Name und Anschrift	Leistungsbeschreibung	Ort der Leistungserbringung / Übermittlungsinstrument
Relaix Networks GmbH <i>Auf der Hüls 172, 52068 Aachen</i>	Colocation: Bereitstellung der physischen Infrastruktur (Stellplatz, Strom, Kühlung, physische Zutrittskontrolle, Netzanbindung) für Server Hardware	Deutschland (Aachen) <u>Kein Drittlandtransfer (EU/EWR)</u>
Google Cloud EMEA Limited <i>70 Sir John Rogerson's Quay, Dublin 2, Irland</i>	1. Infrastructure as a Service (IaaS) 2. Model as a Service (MaaS) über Gemini Enterprise Agent Platform	1. Deutschland (Frankfurt, europe-west3), Belgien (europe-west1) 2. EU <u>EU-U.S. DPF</u>
Microsoft Corporation <i>One Microsoft Way, Redmond, WA 98052, USA</i>	1. Nutzung von Microsoft Azure-Diensten – insbesondere LLMs für die Beantwortung von Prompts, Aufbau einer Vektordatenbank für die Suche sowie automatisierte Übersetzung von Q.wiki-Inhalten. 2. Nutzung von Cloud- und KI-Diensten zur temporären Datenverarbeitung – etwa Sprachverarbeitung, automatische Übersetzung, semantische Suche sowie Erstellung und Optimierung von Prozessen.	EU <u>EU-U.S. DPF</u>
Cloudflare Inc. <i>101 Townsend St., San Francisco, CA 94107, USA</i>	Schutz vor Webanwendungsangriffen (WAF), Abwehr von DDoS-Angriffen sowie Rate Limiting zur Sicherstellung der Ressourcenschonung und Verfügbarkeit	USA <u>EU-U.S. DPF</u>
Mailgun Technologies Inc. <i>112 E. Pecan Street, San Antonio, TX 78205, USA</i>	Q.wiki Mailversand (z. B. Aufgaben, Zurücksetzen des Passwortes)	USA <u>EU-U.S. DPF</u>
Userlane GmbH <i>Rosenheimer Straße 143c, 81671 München</i>	Digitaler Assistent zur softwaregestützten Durchführung von Anwenderschulungen	Deutschland <u>Kein Drittlandtransfer (EU/EWR)</u>
Raintank Inc. d/b/a Grafana Labs <i>165 Broadway, 23rd Floor, New York, NY 10006, USA</i>	Grafana Cloud: Monitoring, Alerting und Visualisierung von Metriken, Logs und Traces zur Sicherstellung von Verfügbarkeit und Betriebssicherheit.	EU / Belgien (Google-Cloud-Region Europe west1, St. Ghislain) <u>EU-U.S. DPF</u>
Freshworks Inc. <i>2950 S. Delaware Street, San Mateo, CA 94403, USA</i>	Ticketing und Wissensdatenbank für den Kundensupport	USA <u>EU-U.S. DPF</u>
Mixpanel Inc. <i>Pier 1, Bay 2, The Embarcadero, San Francisco, CA 94111 USA</i>	Analyse von Nutzungsdaten zur Verbesserung von Q.wiki	USA <u>EU-U.S. DPF</u>
Productboard Inc. <i>333 Bush Street, San Francisco, CA 94104 USA</i>	Verwaltung und Bearbeitung von Kundenfeedback	USA <u>EU-U.S. DPF</u>

Name und Anschrift	Leistungsbeschreibung	Ort der Leistungserbringung / Übermittlungsinstrument
360 Learning SA 37 Rue des Mathurins, Paris, France	Verwaltung und Durchführung von Nutzertrainings	Frankreich <u>Kein Drittlandtransfer (EU/EWR)</u>
Hubspot Inc. 2 Canal Park, Cambridge, MA 02141, United States	Kundenkommunikation und Vertragsmanagement	USA <u>EU-U.S. DPF</u>