**Lizenzbedingungen für die Software as a Service-Lösung mAikit**

## 1. Anwendungsbereich

1.1. Diese Lizenzbedingungen (nachfolgend „**AGB**“) finden ausschließlich Anwendung auf die Zurverfügungstellung der Software as a Service-Lösung „mAikit“ (nachfolgend „**SaaS-Lösung“**) zwischen der QLero GmbH, geschäftsansässig Südliche Münchner Str. 62, 82031 Grünwald (nachfolgend „**Anbieter**“) und deren Kunden (nachfolgend „**Auftraggeber**“). Die Leistungen des Anbieters richten sich ausschließlich an Unternehmer im Sinne des § 14 BGB.

1.2. Entgegenstehende oder von diesen AGB abweichende Geschäftsbedingungen des Auftraggebers werden nur Vertragsbestandteil, soweit der Anbieter ihrer Geltung ausdrücklich zugestimmt hat. Dies gilt insbesondere auch, wenn der Anbieter Leistungen vorbehaltlos ausführt, Zahlungen widerspruchslos entgegennimmt oder den AGB des Auftraggebers nicht ausdrücklich widerspricht.

1.3. Der Anbieter behält sich das Recht vor, diese AGB zu ändern, insbesondere sofern nach Vertragsschluss unvorhersehbare, nicht vom Anbieter zu beeinflussende Änderungen eingetreten sind, wie beispielsweise Gesetzesänderungen, oder Lücken offenbar werden, oder sonstige produktspezifische Anpassungen nötig werden, wodurch das Verhältnis von Leistung und Gegenleistung erheblich gestört wird. In diesem Fall wird der Auftraggeber vier (4) Wochen vor Inkrafttreten der Änderungen durch Mitteilung der neuen AGB per E-Mail oder im Rahmen seines Accounts informiert und zur Zustimmung zu den neuen AGB aufgefordert. Sofern der Auftraggeber den neuen AGB nicht zustimmt, hat der Anbieter ein Sonderkündigungsrecht. Der Anbieter wird den Auftraggeber im Rahmen seiner Mitteilung auf diese Folge ausdrücklich hinweisen.

1.4. Die AGB werden vom Anbieter nach dem Vertragsschluss nicht gespeichert. Der Auftraggeber hat Zugang zur jeweils aktuellen Fassung der AGB im Rahmen seines Accounts.

1.5. Im Einzelfall getroffene, individuelle schriftliche Vereinbarungen zwischen Auftraggeber und Anbieter (einschließlich Nebenabreden, Ergänzungen und Änderungen) haben in jedem Falle Vorrang vor diesen AGB.

## 2. Vertragsschluss und Registrierung

2.1. Die Nutzung der SaaS-Lösung setzt den Abschluss eines Lizenzvertrags zwischen Auftraggeber und Anbieter voraus. Der Lizenzvertrag über die vom Anbieter zu erbringende SaaS-Lösung kommt entweder nach Durchführung des Bestellprozesses und Annahme des Vertragsangebots durch den Anbieter oder mit Annahme des Angebots des Anbieters unter Beifügung bzw. Verweis auf diese AGB durch den Auftraggeber zu Stande.

2.2. Nach Abschluss des Lizenzvertrags erhält der Auftraggeber einen Aktivierungslink zur Registrierung eines Unternehmensaccounts (nachfolgend „Hauptkonto“) und zur Nutzung der SaaS-Lösung. Der Auftraggeber legt dazu eigene Zugangsdaten fest.

2.3. Die Registrierung einer juristischen Person oder einer Personengesellschaft darf nur von einer vertretungsberechtigten natürlichen Person vorgenommen werden, die namentlich zu nennen ist. Der Anbieter darf Registrierungen ablehnen, soweit dafür ein sachlicher Grund

vorliegt, z.B. unrichtige Angaben gemacht werden oder zu befürchten ist, dass den Zahlungspflichten nicht nachgekommen wird.

2.4. Der Auftraggeber ist berechtigt, unter seinem Hauptkonto zusätzliche Accounts für weitere berechtigte Nutzer zu registrieren (nachfolgend „**Unterkonten**"). Der Auftraggeber ist dafür verantwortlich, dass die Unterkonten nur von vertretungsberechtigten Nutzern erstellt und genutzt werden. Der Auftraggeber ist darüber hinaus für alle Handlungen sowohl im Rahmen des Hauptkontos als auch der einzelnen darunter registrierten Unterkonten verantwortlich.

## 3. Bereitstellung der SaaS-Lösung

3.1. Der Anbieter stellt dem Auftraggeber während der Vertragslaufzeit die SaaS-Lösung mittels Zugriffsmöglichkeit auf die Plattform „mAikit" zur Nutzung der Funktionalitäten sowie Speicherplatz für die vom Auftraggeber durch Nutzung der SaaS-Lösung erzeugten und/oder in das Datenmodell eingebrachten Daten nach Maßgabe dieser Bedingungen zur Verfügung.

3.2. Der Leistungsumfang und die wesentlichen Produkteigenschaften der SaaS-Lösung ergeben sich aus der jederzeit abrufbaren Produktbeschreibung. Anderweitige technische Beschreibungen, Datenblätter oder sonstige Erwartungen des Auftraggebers an die SaaS-Lösung und die Leistungen des Anbieters werden nicht Vertragsbestandteil, es sei denn, diese sind ausdrücklich vereinbart.

3.3. Der Anbieter unterstützt den Auftraggeber auf Anfrage bei der Implementierung der SaaS-Lösung und bietet Schulungsleistungen an. Der Auftraggeber kann diese Leistungen auf Anfrage beim Anbieter beauftragen. Nach Annahme des Angebots des Anbieters durch den Auftraggeber wird die jeweils ausgewählte Leistung Vertragsbestandteil zu den genannten Konditionen des Anbieters.

3.4. Der Auftraggeber hat die in der Produktbeschreibung angegebenen Anforderungen an die Nutzung der SaaS-Lösung zu beachten und vollumfänglich sicherzustellen, sowie insbesondere die entsprechenden technischen Voraussetzungen auf eigene Kosten zu schaffen und Systemanforderungen eigenständig umzusetzen.

3.5. Der Auftraggeber ist berechtigt, die SaaS-Lösung für die Dauer von sieben (7) Tagen kostenfrei zu testen. In diesem Zeitraum stehen dem Auftraggeber die Funktionen der SaaS-Lösung vollumfänglich zum Testen zur Verfügung.

3.6. Der Anbieter ist berechtigt, die SaaS-Lösung jederzeit zu aktualisieren sowie weiterzuentwickeln und auf Grund einer geänderten Rechtslage, technischer Entwicklungen oder zur Verbesserung der IT-Sicherheit anzupassen. Der Anbieter wird dabei die berechtigten Interessen des Auftraggebers angemessen berücksichtigen und rechtzeitig über notwendige Updates informieren. Sofern und soweit mit der Bereitstellung einer neuen Version oder eines Updates eine wesentliche Änderung von Funktionalitäten der SaaS-Lösung einhergehen sollte, wird der Anbieter dies dem Auftraggeber spätestens vier (4) Wochen vor dem Wirksamwerden einer solchen Änderung mitteilen. Der Auftraggeber ist berechtigt, einer solchen Änderung zu widersprechen, wodurch der Lizenzvertrag außerordentlich beendet wird. Widerspricht der Auftraggeber der Änderung nicht schriftlich innerhalb einer Frist von vier (4) Wochen ab Zugang der Änderungsmitteilung, wird die Änderung Vertragsbestandteil.

## 4. Einräumung von Nutzungsrechten

4.1. Der Anbieter räumt dem Auftraggeber gegen Zahlung der vereinbarten Vergütung das zeitlich auf die Vertragslaufzeit beschränkte, nicht-ausschließliche, nicht-unterlizenzierbare und nicht übertragbare Recht ein, die SaaS-Lösung für die vereinbarte Anzahl an berechtigen Nutzern nach Maßgabe der nachstehenden Bedingungen zu nutzen.

4.2. Dem Hauptkonto können gem. Ziff. 2.4. weitere Unterkonten für die vereinbarte Anzahl an berechtigten Nutzern zugeordnet werden. Die Anzahl an Unterkonten muss dabei mit der Anzahl der berechtigten Nutzer übereinstimmen. Sofern der Auftraggeber die SaaS-Lösung durch weitere Nutzer nutzen möchte, sind hierfür entsprechende Lizenzen zu beschaffen.

4.3. Der Auftraggeber darf die SaaS-Lösung nur insoweit vervielfältigen, wie dies durch die bestimmungsgemäße Benutzung der SaaS-Lösung abgedeckt ist. Zur notwendigen Vervielfältigung zählt das Laden in den Arbeitsspeicher auf dem Server des Anbieters, **nicht** jedoch die auch nur vorübergehende Installation oder das Speichern auf Datenträgern der vom Auftraggeber eingesetzten Hardware.

4.4. Der Auftraggeber wird die SaaS-Lösung nur für seine internen Unternehmenszwecke einsetzen. Er ist nicht berechtigt, die SaaS-Lösung selbst oder die Rechte daran zu vermieten, zu verleihen, zu verkaufen, Dritten zur Nutzung zu überlassen, abzutreten oder zu übertragen, die SaaS-Lösung zu kopieren oder das Kopieren in Teilen oder als Ganzes zu genehmigen.

4.5. Im Falle der Zurverfügungstellung der SaaS-Lösung zu Testzwecken beschränken sich die Nutzungsrechte des Auftraggebers auf solche Handlungen, die der Feststellung der Funktionen der SaaS-Lösung und der Prüfung der Eignung für den Auftraggeber dienen; insbesondere ein produktiver Betrieb der SaaS-Lösung ist unzulässig. Nach Ablauf des 7-tägigen Testzeitraums werden dem Auftraggeber die Nutzungsrechte gemäß der vorstehenden Ziffern eingeräumt, sofern der Auftraggeber nicht innerhalb des Testzeitraums die Kündigung des Lizenzvertrags gem. Ziff. 16.1. erklärt hat.

4.6. Jeder ergänzende Programmcode (z.B. Update, Upgrade), der dem Auftraggeber zum Zwecke der Fehlerbehebung oder im Rahmen von Wartung/Support zur Verfügung gestellt wird, wird als Bestandteil der jeweils überlassenen SaaS-Lösung betrachtet und unterliegt den Bedingungen dieser AGB, soweit nichts anderes vereinbart wurde.

4.7. Hinsichtlich der Bestandteile des in der SaaS-Lösung beinhalteten KI-Systems mit allgemeinem Verwendungszweck, das nach der zum Zeitpunkt des Vertragsschlusses gemeinsamen Annahme der Parteien keinen urheberrechtlichen Schutz genießt, räumt der Anbieter dem Auftraggeber die tatsächliche Nutzungsbefugnis ein. Hierbei handelt es sich im Wesentlichen um das KI-System mit allgemeinem Verwendungszweck (nachfolgend „**Datenmodell**“) und die auf dieser Grundlage zur Verfügung gestellten Vorhersagen des Datenmodells. Sofern an diesen nicht geschützten Bestandteilen gleichwohl urheberrechtliche Schutzrechte bestehen oder zukünftig entstehen sollten, finden die vorstehenden Regelungen dieser Ziff. 4 entsprechende Anwendung.

## 5. Pflichten des Auftraggebers

5.1. Der Auftraggeber stellt sicher, dass alle von ihm gemachten Angaben und übermittelten Informationen

vollständig, aktuell und korrekt sind. Der Auftraggeber wird seine Angaben im Rahmen des Unternehmensaccounts stets aktuell halten und ist zur unverzüglichen Aktualisierung bei Änderungen verpflichtet.

5.2. Zugangsdaten wird der Auftraggeber vertraulich behandeln und nur an berechtigte Mitarbeiter weitergeben. Der Auftraggeber wird durch geeignete Maßnahmen sicherstellen, dass unbefugte Dritte nicht auf die SaaS-Lösung zugreifen können. Der Auftraggeber ist insbesondere verpflichtet, alle Passwörter zur Nutzung der SaaS-Lösung auf eigene Kosten vor dem unberechtigten Zugriff Dritter zu schützen und seine Mitarbeiter hierzu entsprechend zu verpflichten. Der Auftraggeber ist verpflichtet, dem Anbieter jeden unberechtigten Zugriff bzw. dessen Versuch unverzüglich mitzuteilen.

5.3. Im Rahmen der Nutzung der SaaS-Lösung ist es dem Auftraggeber insbesondere untersagt,

a) die SaaS-Lösung zu verwenden, um aus den gewonnen Erkenntnissen eigene Programme zu entwickeln (sog. „Reverse Engineering“),

b) die SaaS-Lösung auf eine Art und Weise zu verwenden, die gegen behördliche Vorgaben oder gesetzliche Rahmenbedingungen verstößt,

c) Programme, insbesondere schadhafte Programme, die den Betrieb der SaaS-Lösung schädigen, überlasten oder stören könnten, zu verwenden oder zu übermitteln.

5.4. Der Auftraggeber übernimmt die volle Verantwortung für von ihm hochgeladene Inhalte und bereitgestellte Daten.

5.5. Der Auftraggeber wird den Anbieter von sämtlichen Ansprüchen Dritter auf erstes Anfordern freistellen, die auf einer unzulässigen Verwendung der SaaS-Lösung beruhen.

5.6. Der Auftraggeber räumt dem Anbieter das Recht zur Überprüfung der Einhaltung der Vertragsbedingungen ein. Der Auftraggeber wird den Anbieter oder ein zur Verschwiegenheit verpflichteter Dritter bei der Überprüfung unterstützen, insbesondere Auskunft erteilen und Einsicht in für die Überprüfung relevante Unterlagen und Dokumente (wie etwa Reports) ermöglichen. Sofern sich bei der Überprüfung ein Verstoß gegen die Vertragsbedingungen ergeben sollte, so verpflichtet sich der Auftraggeber sowohl zur Nachzahlung der jeweiligen Vergütung als auch zur Übernahme der für die Prüfung entstandenen Kosten. Alle sonstigen Rechte bleiben vorbehalten.

5.7. Der Auftraggeber wird in eigener Verantwortung regelmäßig angemessene Datensicherungen in Bezug auf die mittels der SaaS-Lösung erstellten oder verarbeiteten Daten vornehmen.

5.8. Der Auftraggeber stellt sicher, dass die für die Nutzung der SaaS-Lösung erforderliche ~~KI-~~Kompetenz in seinem Unternehmen vorhanden ist.

5.9. Soweit der Auftraggeber seinen Mitwirkungspflichten nicht, nicht ordnungsgemäß oder nicht rechtzeitig nachkommt und dies Auswirkungen auf die Leistungserbringung des Anbieters hat, ist der Anbieter für die dem Auftraggeber hieraus entstehenden Nachteile nicht verantwortlich. Ferner ist der Anbieter zur Aussetzung seiner Leistungen berechtigt, bis der Auftraggeber seinen Mitwirkungspflichten vollständig, ordnungsgemäß und rechtzeitig nachkommt. Den hierdurch verursachten Mehraufwand wird der Anbieter - unbeschadet weiterer Rechte - dem Auftraggeber gesondert in Rechnung

stellen. Darüber hinaus hat der Auftraggeber dem Anbieter auf Nachweis etwaig entstandene Auslagen zu erstatten.

## 6. Vergütung, Zahlungsbedingungen

6.1. Die Vergütung für die Nutzung der SaaS-Lösung (nachfolgend „Lizenzgebühren“) richtet sich nach der jeweils aktuellen Preisliste und dem Angebot des Anbieters. Es handelt sich dabei um Nettopreise zzgl. der jeweils geltenden gesetzlichen Mehrwertsteuer. Sofern der Auftraggeber im Einzelfall Steuerschuldner ist, gilt insoweit das Reverse-Charge-Verfahren.

6.2. Nach Ablauf des kostenfreien 7-tägigen Testzeitraums erfolgt die Zahlung der Lizenzgebühren über die vom Auftraggeber ausgewählte Zahlungsmethode im Wege der Vorauszahlung. Für einzelne Zahlungsmethoden werden entsprechende Zahlungsdienstleister eingesetzt, deren Nutzungsbedingungen jeweils gelten. Die Lizenzgebühren für die Nutzung des Hauptkontos sind nach Wahl des Auftraggebers entweder monatlich oder jährlich im Voraus fällig.

6.3. Dem Hauptkonto ist ein entsprechendes Credit-Volumen für die Nutzung von Fragen/Interaktionen (wie beispielsweise Anfragen) im Rahmen der SaaS-Lösung durch den Auftraggeber hinterlegt. Credits aus den Unterkonten werden dem Hauptkonto gutgeschrieben. Die Abrechnung erfolgt nutzerbasiert je Anzahl und Umfang von Fragen/Interaktionen. Dem Auftraggeber wird eine Verbrauchsübersicht im Dashboard der SaaS-Lösung angezeigt. Die Nutzer der Unterkonten können dabei sehen, welche Interaktion wie viele Credits verbraucht hat. Der Auftraggeber wird bei niedrigem Credit-Stand informiert und kann Credit-Pakete jederzeit manuell nachbuchen. Die Abrechnung erfolgt monatlich über die im Hauptkonto hinterlegte Zahlungsmethode. Vorhandene Restcredits aus den Haupt- und Unterkonten verfallen am Ende der Vertragslaufzeit. Bei Kündigung eines Unterkontos verfallen die zugeordneten Credits zum entsprechenden Monatsende. Während der Vertragslaufzeit werden Restcredits aus dem Vormonat in den Folgemonat übertragen. Es erfolgt keine Erstattung nicht genutzter Credits nach Laufzeitende.

6.4. Im Falle von wiederkehrenden Zahlungsverpflichtungen kündigt der Anbieter dem Auftraggeber Preisänderungen mindestens drei (3) Monate vor Ende der Vertragslaufzeit an. Im Falle einer Preiserhöhung ist der Auftraggeber binnen vier (4) Wochen nach Zugang der Mitteilung berechtigt, der Preiserhöhung zu widersprechen. Sofern der Auftraggeber nicht widerspricht, gelten die neuen Preise für die neue Vertragslaufzeit und die Folgejahre bis zu einer etwaigen weiteren Preisänderung. Widerspricht der Auftraggeber, ist der Anbieter berechtigt das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von drei (3) Monaten zum Ende der Vertragslaufzeit zu kündigen.

6.5. Mit Ablauf der vereinbarten Zahlungsfrist/en kommt der Auftraggeber in Verzug, ohne dass es einer Mahnung durch den Anbieter bedarf. Der fällige Betrag ist während des Verzuges mit dem jeweils geltenden gesetzlichen Verzugszins zu verzinsen. Die Geltendmachung eines weitergehenden Verzugsschadens sowie der Pauschale gem. § 288 Abs. 5 BGB bleiben unberührt.

## 7. Gewährleistung bei Sach- und Rechtsmängeln

7.1. Im Hinblick auf die Gewährung der Nutzung der SaaS-Lösung gelten die Vorschriften der §§ 535 ff. BGB.

7.2. Minderungen der Vergütung darf der Auftraggeber nicht dadurch geltend machen, dass er den Minderungsbetrag von der zu zahlenden Vergütung eigenständig abzieht. Unberührt hiervon bleibt der Rückerstattungsanspruch des Auftraggebers hinsichtlich der zu viel gezahlten Vergütung im Falle einer berechtigten Minderung.

7.3. Die Gewährleistung für nur unerhebliche Minderungen der Tauglichkeit der SaaS-Lösung wird ausgeschlossen. Die verschuldensunabhängige Haftung des Anbieters für bereits bei Vertragsschluss vorhandene Mängel gem. § 536a Abs. 1 BGB wird ebenfalls ausgeschlossen.

7.4. Sofern Dritte wegen der Verletzung von Rechten gegen den Auftraggeber Ansprüche geltend machen, wird der Auftraggeber den Anbieter hierüber unverzüglich schriftlich oder in Textform informieren. Der Auftraggeber ist nicht berechtigt, ein Anerkenntnis gegenüber dem Dritten abzugeben, und er wird dem Anbieter ausdrücklich alle Abwehrmaßnahmen und Vergleichshandlungen vorbehalten. Der Anbieter ist nach eigener Wahl berechtigt entweder die SaaS-Lösung so zu verändern, dass das Recht des Dritten nicht mehr verletzt wird, oder dem Auftraggeber die benötigte Befugnis zur Nutzung der SaaS-Lösung zu verschaffen. Die Selbstvornahme durch den Auftraggeber oder von ihm beauftragter Dritter ist ausgeschlossen.

7.5. Im Falle der Mangelhaftigkeit von verwendeter Fremd-Software, die der Anbieter zum Zwecke der Leistungserbringung einsetzt und deren Mängel der Anbieter nicht selbst beheben darf, besteht die Pflicht des Anbieters zur Mängelbeseitigung in der Geltendmachung der Ansprüche gegenüber den jeweiligen Lizenzgebern.

## 8. Service Levels, Störungen

8.1. Der Anbieter stellt eine durchschnittliche jährliche Verfügbarkeit der SaaS-Lösung am Übergabepunkt von 96 % sicher. Übergabepunkt ist der Routerausgang des Rechenzentrums, in dem der Server der SaaS-Lösung des Anbieters steht.

8.2. Unter Verfügbarkeit verstehen die Parteien die technische Nutzbarkeit der SaaS-Lösung am Übergabepunkt zum Gebrauch durch den Auftraggeber. Wartungszeiten, Zeiten der Störung unter Einhaltung der vereinbarten Beseitigungszeit sowie nicht dem Anbieter zurechenbare Zeiten der Störung von erforderlicher technischer Infrastruktur beim Auftraggeber gelten als Zeiten der Verfügbarkeit der SaaS-Lösung. Zeiten unerheblicher Störungen bleiben bei der Berechnung der Verfügbarkeit außer Betracht. Für den Nachweis der Verfügbarkeit sind die Messinstrumente des Anbieters im Rechenzentrum maßgeblich.

8.3. Der Auftraggeber hat jegliche Störungen unverzüglich an den Anbieter per E-Mail oder telefonisch zu melden.

8.4. Störungsbehebungen erfolgen innerhalb folgender Servicezeiten: Montag bis Freitag jeweils zwischen 9 Uhr und 17 Uhr (unter Ausnahme gesetzlicher Feiertage am Sitz des Anbieters). Für die Servicezeiten gilt die Zeitzone am Sitz des Anbieters.

8.5. Der Anbieter nimmt in eigenem Ermessen unter Berücksichtigung der Interessen des Auftraggebers eine Einordnung der auftretenden Störung in entsprechende Kategorien nach Maßgabe der folgenden Regelungen vor.

8.6. Auf sämtliche vom Auftraggeber mitgeteilten Störungen wird der Anbieter binnen vier (4) Stunden ab Eingang der Meldung der Störung reagieren, sofern die Meldung innerhalb der Servicezeiten erfolgt. Außerhalb der Servicezeiten wird der Anbieter binnen zwölf (12) Stunden reagieren. Der Anbieter teilt dem Auftraggeber jeweils mit, bis wann die Behebung der Störung voraussichtlich erfolgen wird. Sofern absehbar ist, dass dies nicht innerhalb der vom Anbieter mitgeteilten Zeitspanne möglich ist, wird der Anbieter den Auftraggeber hierüber unverzüglich informieren und die voraussichtliche Überschreitung der Zeitspanne mitteilen.

8.7. Die Beseitigung von unerheblichen Störungen liegt im Ermessen des Anbieters und kann durch Updates oder neue Programmversionen, die daneben auch neue Funktionen enthalten können (Upgrades), erfolgen.

## 9. Support und Wartung

9.1. Der Anbieter richtet für Anfragen des Auftraggebers zu Funktionen der SaaS-Lösung einen teilweise oder vollständig KI-gestützten Support ein. Anfragen können an die auf der Website des Anbieters angegebene E-Mail-Adresse oder an die zur Verfügung gestellte Chatmöglichkeit gerichtet werden. Die Nutzer werden darüber informiert, wenn KI-gestützter Support eingesetzt wird. Die Anfragen werden grundsätzlich in zeitlicher Reihenfolge ihres Eingangs bearbeitet. Die auf Basis der Informationen mittels des KI-gestützten Supports zur Verfügung gestellten Antworten stellen lediglich Hilfestellungen und keine Rechtsberatung dar.

9.2. Der Anbieter ist berechtigt, regelmäßige Wartungen vorzunehmen. Diese finden in der Zeit von 17 bis 22 Uhr und damit grundsätzlich außerhalb der üblichen Geschäftszeiten statt, es sei denn, die Wartung muss aus dringenden betrieblichen oder anderen zwingenden Gründen zu einer anderen Zeit vorgenommen werden.

9.3. Sofern erforderlich, werden darüber hinaus gehende Wartungen grundsätzlich achtundvierzig (48) Stunden im Voraus per E-Mail angekündigt.

9.4. Wenn und soweit der Auftraggeber in angekündigten Zeiten der Nichtverfügbarkeit die SaaS-Lösung nutzen kann, so besteht hierauf kein Rechtsanspruch.

## 10. Leistungsausschlüsse

10.1. Bei der SaaS-Lösung handelt es sich um ein technisches Werkzeug, das Informationen in strukturierter Form bereitstellt. Diese Informationen basieren auf den Daten des Auftraggebers und ersetzen weder individuelle Rechtsberatung noch begründen sie einen Anspruch auf Vollständigkeit, Richtigkeit oder Aktualität. Der Auftraggeber trägt die Verantwortung für die auf Grundlage der bereitgestellten Informationen getroffenen wirtschaftlichen, organisatorischen und rechtlichen Entscheidungen.

10.2. Der Auftraggeber erkennt an, dass es sich bei den mittels der SaaS-Lösung zur Verfügung gestellten Informationen lediglich um Annahmen handelt, die auf Grund von Wahrscheinlichkeiten getroffen wurden, und deren Qualität insbesondere von der Qualität der vom Auftraggeber zur Verfügung gestellten Daten abhängt. Zu den vertragsgegenständlichen Leistungen zählt daher explizit nicht die Richtigkeit, Vollständigkeit oder Mangelfreiheit von Schutzrechten Dritter in Bezug auf diese Annahmen.

## 11. Höhere Gewalt

11.1. Schwerwiegende Ereignisse, wie insbesondere höhere Gewalt, Arbeitskämpfe, Unruhen, behördliche Maßnahmen und sonstige unvorhersehbare Ereignisse, welche der Anbieter nicht zu vertreten hat, (nachfolgend insgesamt als „**höhere Gewalt**“ bezeichnet) befreit diesen für die Dauer der höheren Gewalt im Umfang ihrer Wirkung von seinen vertraglichen Pflichten.

11.2. In diesen Fällen ist der Anbieter berechtigt, die Erbringung der vertragsgegenständlichen Leistungen um die Dauer der Behinderung zuzüglich einer angemessenen Anlaufzeit hinauszuschieben.

## 12. Haftung und Freistellung

12.1. Der Anbieter haftet unbeschränkt für Schäden, die auf Vorsatz oder grober Fahrlässigkeit beruhen, für Schäden auf Grund der Verletzung des Lebens, des Körpers oder der Gesundheit sowie im Falle zwingender gesetzlicher Vorschriften, insbesondere der Haftung nach dem Produkthaftungsgesetz (ProdHG), der Übernahme einer Garantie oder im Falle eines arglistig verschwiegenen Mangels.

12.2. Der Anbieter haftet im Falle leichter Fahrlässigkeit für die Verletzung wesentlicher Vertragspflichten. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf. Die Haftung ist insoweit jedoch auf den vorhersehbaren, vertragstypischen Schaden beschränkt.

12.3. Die Haftung für einen möglichen Verlust oder eine Zerstörung von Daten ist auf den Wiederherstellungsaufwand beschränkt, der bei ordnungsgemäßer Datensicherung entstanden wäre.

12.4. Die vorstehenden Haftungsregelungen gelten auch hinsichtlich der Haftung des Anbieters für seine Erfüllungsgehilfen und gesetzlichen Vertreter.

12.5. Im Falle, dass der Anbieter auf Grund eines Schadens in Anspruch genommen wird, der durch Informationen, insbesondere Daten des Auftraggebers, sowie unsachgemäße Verwendung der bereitgestellten SaaS-Lösung verursacht werden, wird der Auftraggeber den Anbieter von allen Ansprüchen, die auf Grund dessen gegen den Anbieter geltend gemacht werden, auf erste Anforderung freistellen und schadlos halten.

12.6. Der Anbieter stellt einen ausreichenden Versicherungsschutz zur Deckung möglicherweise entstehender Schäden, die im Zusammenhang mit dem zwischen den Parteien geschlossenen Lizenzvertrag stehen und für die der Anbieter nach dieser Ziff. 12 einzustehen hat, sicher.

## 13. Geheimhaltung

13.1. Die Parteien verpflichten sich, sämtliche im Rahmen der Zusammenarbeit erhaltenen vertraulichen Informationen sowie Betriebs- und Geschäftsgeheimnisse der anderen Partei Dritten gegenüber geheim zu halten, solange und soweit diese Informationen geheim sind.

13.2. Als vertrauliche Informationen des Anbieters gelten insbesondere alle Produkte, Dienste, Techniken und Know-How des Anbieters, insbesondere zu dem in der SaaS-Lösung beinhalteten Datenmodell und dessen Selbstoptimierung sowie der Verlauf und die Ergebnisse einer Anlernphase des Datenmodells und dessen Vorhersagen, sowie sämtliche dem Auftraggeber im Rahmen des Vertragsverhältnisses bzw. dessen Durchführung bekannt wer-

denden Informationen, unabhängig davon, ob diese schriftlich, mündlich oder in elektronischer Form übermittelt wurden. Sofern eine vertrauliche Information nicht den Anforderungen an ein Geschäftsgeheimnis nach GeschGehG genügen sollte, unterfällt diese Information gleichwohl den Regelungen dieser Ziff. 13.

13.3. Die Geheimhaltungspflicht gilt nicht für Informationen, die bereits vor Beginn der Zusammenarbeit allgemein bekannt waren, auf andere Weise allgemein bekannt werden, ohne dass es sich dabei um eine Verletzung dieser Geheimhaltungspflicht handelt, oder auf deren vertrauliche Behandlung die jeweils andere Partei schriftlich verzichtet hat.

13.4. Die Geheimhaltungspflicht gilt während der Laufzeit des Lizenzvertrags sowie nach Beendigung für die Dauer von weiteren 5 Jahren.

13.5. Die Parteien stellen sicher, dass ihre Mitarbeiter, Erfüllungsgehilfen sowie sonstige eingesetzte Dritte ebenfalls zur Geheimhaltung nach dieser Ziff. 13 verpflichtet werden.

13.6. Jeder schuldhafte Verstoß gegen die in dieser Ziff. 13. enthaltenen Geheimhaltungsverpflichtung durch den Auftraggeber berechtigt den Anbieter, eine in jedem Einzelfall nach billigem Ermessen der Höhe nach angemessene Vertragsstrafe zu verlangen, die vom zuständigen Gericht im Streitfalle auf deren Rechtmäßigkeit überprüft werden kann. Die Geltendmachung eines weitergehenden Schadens bleibt vorbehalten. Eine gezahlte Vertragsstrafe wird auf etwaige Schadensersatzansprüche aus derselben Pflichtverletzung angerechnet. Die Vertragsstrafe stellt dabei die Mindesthöhe des Schadens dar. Der Auftraggeber ist jedoch berechtigt, den Nachweis eines niedrigeren Schadens zu erbringen.

## 14. Nennung als Referenzkunde

Der Auftraggeber gestattet dem Anbieter die Nennung als Referenzkunde auf seiner Website und in anderen Medien wie Print- und Digitalmedien. Dazu räumt der Auftraggeber dem Anbieter das jederzeit für die Zukunft widerrufliche, einfache, zeitlich unbeschränkte Recht zur Nutzung des Unternehmensnamens und des Logos des Auftraggebers in Werbematerialien und auf der Website des Anbieters ein.

## 15. Datenschutz

15.1. Der Auftraggeber trägt die Verantwortung für die Einhaltung aller datenschutzrechtlichen Bestimmungen zur Verarbeitung von personenbezogenen Daten. Im Falle der Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO gilt die Auftragsverarbeitungsvereinbarung des Anbieters in Anlage 1.

15.2. Der Anbieter ist berechtigt, Daten in anonymisierter Form für Analysezwecke und zur Fehlerbehebung zu verwenden.

## 16. Vertragslaufzeit und Beendigung

16.1. Die Laufzeiten des Haupt- und der Unterkonten richten sich jeweils nach dem ausgewählten Angebot des Anbieters. Die Laufzeit des Hauptkontos beginnt mit Ablauf des 7-tägigen Testzeitraums, sofern der Auftraggeber den Lizenzvertrag nicht innerhalb des Testzeitraums kündigt. Im Anschluss an die Erstlaufzeit verlängert sich der Lizenzvertrag entsprechend um die vereinbarte Dauer, sofern er nicht von einer Partei mit entsprechender Frist zum Ende der jeweiligen Laufzeit gekündigt wird. Eine Kündigung von Unterkonten ist durch

den Nutzer des Hauptkontos jeweils zum Monatsende möglich.

16.2. Das Recht zur fristlosen Kündigung aus wichtigem Grunde bleibt unberührt. Ein wichtiger Grund für den Anbieter liegt unter anderem dann vor, wenn sich der Auftraggeber mit der Zahlung der Vergütung mehr als sechzig (60) Tage im Verzug befindet oder gegen wesentliche Vertragspflichten, insbesondere gegen Bestimmungen zu Nutzungsrechten, verstößt und diesen Verstoß nicht innerhalb von dreißig (30) Tagen nach einer Abmahnung durch den Anbieter beseitigt. Das Recht des Auftraggebers zur außerordentlichen Kündigung gem. § 543 Abs. 2 S. 1 Nr. 1 BGB ist ausgeschlossen.

16.3. Reicht der Regelungsgehalt einzelner Vorschriften dieser Lizenzbedingungen über das Vertragsende hinaus, bleiben diese Vorschriften insoweit auch nach Vertragsbeendigung wirksam.

16.4. Kündigungen können direkt im Hauptkonto vorgenommen werden.

16.5. Nach Vertragsbeendigung enden die Nutzungsrechte des Auftraggebers automatisch, ohne dass es einer Erklärung des Anbieters bedarf.

16.6. Nach Vertragsbeendigung wird der Anbieter dem Auftraggeber seine Daten auf Verlangen binnen einem (1) Monat in einem gängigen Datenformat zur Verfügung stellen.

Unbeschadet der vorstehenden Regelungen zur Beendigung des Lizenzvertrages und den rechtlichen Folgen richten sich im Falle eines Wechsel- oder Datenlöschungsverlangens nach Art. 25 Data Act die Beendigung des Vertrages und die rechtlichen Folgen nach **Anlage 2** (Cloud-Switching). Darin werden auch die zum Cloud-Switching erforderlichen Informationen als Anhang bereitgestellt.

## 17. Schlussbestimmungen

17.1. Mündliche oder schriftliche Nebenabreden bestehen nicht. Änderungen und Ergänzungen des Lizenzvertrags bedürfen der Schriftform, soweit nicht eine Individualvereinbarung getroffen wurde. Das gilt auch für die Aufhebung dieses Schriftformerfordernisses.

17.2. Für sämtliche Streitigkeiten aus und in Zusammenhang mit diesen Bedingungen wird als ausschließlicher Gerichtsstand München vereinbart, soweit die Parteien Kaufleute sind.

17.3. Auf diese Bedingungen findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG) Anwendung.

17.4. Sollte eine Bestimmung dieser Bedingungen ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Bedingungen sowie der verbleibenden Bestimmungen des Lizenzvertrags im Übrigen nicht berührt. Die Parteien werden sich bemühen, eine wirksame und durchführbare Bestimmung zu vereinbaren, die dem verfolgten wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. Dies gilt gleichermaßen im Falle einer Regelungslücke.

mAikit.AI

**Anlage 1 - Auftragsverarbeitungsvereinbarung gem. Art. 28 DSGVO („AVV“)**

**Präambel**

Diese Vereinbarung legt die Rechte und Pflichten des Anbieters als Auftragsverarbeiter (nachfolgend „**Auftragnehmer**“) und des Auftraggebers als Verantwortlicher im Rahmen der Verarbeitung von personenbezogenen Daten im Auftrag gemäß Art. 28 der EU-Datenschutzgrundverordnung (nachfolgend „**DSGVO**“) fest. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

## § 1 Gegenstand und Dauer der Verarbeitung

(1) Der Gegenstand der Verarbeitung ergibt sich aus dem zwischen den Parteien geschlossenen Lizenzvertrag, auf den im Folgenden Bezug genommen (nachfolgend „**Hauptvertrag**“).

(2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

(3) Soweit die Laufzeit des Hauptvertrags beendet sein sollte, gilt diese Vereinbarung unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

## § 2 Art der Daten und Zweck der Verarbeitung

(1) Der Auftragnehmer erbringt für den Auftraggeber die Leistungen gemäß des Hauptvertrags, insbesondere die Zurverfügungstellung einer Software-Lösung als Software-as-a-Service und damit in Zusammenhang stehende Leistungen. Darüber hinaus erbringt der Auftragnehmer Wartungs- und Supportleistungen für den Auftraggeber, wodurch die Möglichkeit des Zugriffs auf die nachstehend genannten Arten personenbezogener Daten besteht.

(2) Gegenstand der Verarbeitung personenbezogener Daten können dabei die folgenden Datenarten/-kategorien sein:

- allgemeine Personendaten (v.a. Name, Vorname)
- Kommunikationsdaten (v.a. E-Mail-Adresse, Abteilung)
- Zahlungsdaten (...)
- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen die folgenden:
- Beschäftigte des Auftraggebers
- Vertragspartner des Auftraggebers

## § 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer versichert, dass ihm die einschlägigen, geltenden Datenschutzvorschriften bekannt sind und er jederzeit die Grundsätze zur ordnungsgemäßen Verarbeitung personenbezogener Daten beachtet. Diese Vereinbarung entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten grundsätzlich nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Die anfänglichen Weisungen des Auftraggebers werden durch diese Vereinbarung und den Hauptvertrag festgelegt. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften.

(3) Der Auftragnehmer wird die Daten für keine anderen als die festgelegten Zwecke verwenden.

(4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung der Daten die Vertraulichkeit zu wahren und setzt bei der Erbringung seiner Leistungen nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

(5) Die Parteien arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung und die Verarbeitung der Daten des Auftraggebers beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten nach dieser Vereinbarung beim Auftragnehmer ermittelt.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technisch-organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen sichergestellt ist.

(8) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnisnahme an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere gem. Art. 33, 34 DSGVO nachkommen kann. Er wird über den gesamten Vorgang eine Dokumentation erstellen, die er dem Auftraggeber auf Nachfrage zur Kenntnisnahme und für weitere Maßnahmen übermittelt.

(9) Der Auftragnehmer verpflichtet sich, den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung zu stellen.

(10) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, wird der Auftragnehmer den Auftraggeber auf dessen Kosten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen. Dies gilt gleichermaßen für eine ggf. bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde. Die Parteien werden sich über die Modalitäten und Konditionen im Einzelfall schriftlich oder in Textform verständigen.

## § 4 Technisch-organisatorische Maßnahmen („TOMs“)

(1) Der Auftragnehmer verpflichtet sich, in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutze der personenbezogenen Daten zu ergreifen, die im Auftrag des Auftraggebers verarbeitet werden. Die Dokumentation der technisch-organisatorischen Maßnahmen wird zum Zeitpunkt des Vertragsschlusses in **Anhang 1** verbindlich zwischen den Parteien festgelegt.

(2) Die in Anhang 1 dargestellten technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, entsprechend angepasste Maßnahmen in Zukunft umzusetzen, wobei das Sicherheitsniveau der vorliegend festgelegten Maßnahmen nicht unterschritten werden darf. Der Auftragnehmer wird sämtliche Änderungen dokumentieren und den Auftraggeber über wesentliche Änderungen unverzüglich in Kenntnis setzen.

## § 5 Umgang mit Rechten der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anfragen seitens betroffener Personen in Bezug auf deren Datenschutzrechte.

(2) Der Auftragnehmer wird Daten, die im Auftrag verarbeitet werden, nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers beauskunften, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich in Ausübung ihrer Datenschutzrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

## § 6 Einsatz von Unterauftragnehmern

(1) Der Auftragnehmer ist berechtigt, Unterauftragnehmer als weitere Auftragsverarbeiter im Rahmen der Verarbeitung personenbezogener Daten einzusetzen. Der Auftraggeber wird den Einsatz der in **Anhang 2** aufgeführten Unterauftragnehmer gestatten.

(2) Die Auslagerung auf weitere Unterauftragnehmer sowie jeder Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmer ist zulässig, soweit:
   (a) der Auftragnehmer eine solche Auslagerung bzw. den Wechsel dem Auftraggeber mit einer Frist von vier (4) Wochen vorab schriftlich oder in Textform anzeigt und
   (b) der Auftraggeber nicht innerhalb von zwei (2) Wochen nach Erhalt der Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
   (c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 - 4 DSGVO mit dem Unterauftragnehmer besteht.

(3) Im Falle eines Einspruchs des Auftraggebers gegen eine solche Auslagerung bzw. gegen den Wechsel eines Unterauftragnehmers hat der Auftragnehmer das Recht zur außerordentlichen Kündigung dieser Vereinbarung und des Hauptvertrags aus wichtigem Grund.

(4) Der Auftragnehmer wird die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer unter Berücksichtigung des jeweiligen Risikos vor Beginn der Verarbeitung personenbezogener Daten und sodann regelmäßig kontrollieren. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung.

(5) Sofern der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR erbringt, wird der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch geeignete Maßnahmen, insbesondere durch angemessene Datenschutzgarantien, sicherstellen.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers schriftlich oder in Textform.

(7) Im Sinne der vorstehenden Regelungen handelt es sich bei Unterauftragsverhältnissen um solche Leistungen, die sich unmittelbar auf die hauptvertragliche Leistungserbringung beziehen. Hierunter fallen grundsätzlich nicht Nebenleistungen wie z.B. Telekommunikationsdienstleistungen, Post-/ Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach dieser Vereinbarung stehen.

## § 7 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat ein umfassendes Weisungsrecht hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag.

(2) Weisungen werden grundsätzlich in Textform erteilt.

(3) Der Auftraggeber benennt auf Anforderung des Auftragnehmers eine weisungsbefugte Kontaktperson sowie deren Kontaktdaten und teilt Änderungen unverzüglich mit.

(4) Bis zur Benennung einer solchen Kontaktperson gelten Weisungen als wirksam, wenn sie durch eine vertretungsberechtigte Person des Auftraggebers oder durch eine von ihr nachweislich autorisierte Person erteilt werden.

(5) Eine Änderung von befugten Personen und/oder deren Kontaktdaten ist der jeweils anderen Partei unverzüglich schriftlich oder in Textform mitzuteilen.

(6) Der Auftraggeber ist verpflichtet, alle Aufträge, Teilaufträge oder Weisungen in dokumentierter Form, d.h. mindestens in Textform, zu erteilen. Nur in dringenden Ausnahmen dürfen Weisungen mündlich erteilt werden; solche Weisungen hat der Auftraggeber unverzüglich und in entsprechender Weise dokumentiert zu bestätigen.

(7) Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich zu informieren, sofern und soweit er Fehler oder Unregelmäßigkeiten im Rahmen der Auftragsverarbeitung feststellt.

(8) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften zum Datenschutz sowie die vertraglichen Vereinbarungen, insbesondere die vollständige Umsetzung der festgelegten technisch-organisatorischen Maßnahmen und deren Wirksamkeit, beim Auftragnehmer in angemessenem Umfang selbst oder durch einen im Einzelfall zu benennende Prüfer zu kontrollieren. Kontrollen sind insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie durch Kontrollen vor Ort möglich. Der Auftragnehmer ist verpflichtet, notwendige Auskünfte zu erteilen und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(9) Sofern Kontrollen beim Auftragnehmer vor Ort erforderlich sein sollten, werden diese ohne Störung des Geschäftsbetriebs erfolgen. Solche Kontrollen finden maximal ein (1) Mal jährlich und ausschließlich nach angemessener Vorankündigung während der üblichen Geschäftszeiten des Auftragnehmers statt.

## § 8 Datenverarbeitung außerhalb EU/EWR

(1) Sofern eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erforderlich sein sollte, wird der Auftragnehmer die Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO sicherstellen.

(2) Der Auftraggeber gestattet die Datenübermittlung in ein Drittland an die ggf. in Anhang 2 genannten Empfänger. Aus dem Anhang haben sich die vom Auftraggeber genehmigten Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung zu ergeben.

(3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung der Regelungen nach Kapitel V der DSGVO allein verantwortlich.

## § 9 Beendigung der Verarbeitung im Auftrag

(1) Nach Beendigung der Zusammenarbeit wird der Auftragnehmer auf Verlangen des Auftraggebers die personenbezogenen Daten gemäß der vereinbarten Aufbewahrungsfrist an den Auftraggeber übergeben und anschließend von den Servern löschen. Dieses Verlangen hat der Auftraggeber binnen vier (4) Wochen nach Beendigung der Zusammenarbeit auszuüben. Die Löschung erfolgt dergestalt, dass eine Wiederherstellung mit vertretbarem Aufwand unmöglich ist.

(2) Der Auftragnehmer wird die Löschung auch gegenüber seinen Unterauftragnehmern sicherstellen, soweit dies vertraglich möglich und rechtlich zulässig ist.

(3) Der Auftragnehmer ist zum Nachweis der ordnungsgemäßen Löschung verpflichtet und wird diesen dem Auftraggeber entsprechend vorlegen. Der Auftragnehmer ist berechtigt, Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen auch über die Laufzeit dieser Vereinbarung hinaus aufzubewahren.

## § 10 Schlussbestimmungen

(1) Diese Vereinbarung gilt vorrangig, auch soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, es sei denn, die Parteien haben ausdrücklich etwas anderes vereinbart.

(2) Diese Vereinbarung ersetzt alle mündlichen oder schriftlich getroffenen Abreden, die zuvor zwischen den Parteien hinsichtlich des Gegenstands der Verarbeitung getroffen wurden.

(3) Darüber hinaus gehende mündliche oder schriftliche Nebenabreden zu dieser Vereinbarung wurden nicht getroffen.

(4) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform, soweit nicht eine Individualvereinbarung getroffen wurde. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(5) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Vereinbarung sowie der verbleibenden Bestimmungen im Übrigen nicht berührt. Die Parteien werden sich bemühen, eine wirksame und durchführbare Bestimmung zu vereinbaren, die dem verfolgten wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. Dies gilt gleichermaßen im Falle einer Regelungslücke.

(6) Die folgenden Anhänge zu dieser Vereinbarung sind integraler und wesentlicher Vertragsbestandteil:
**Anhang 1:** Technisch-organisatorische Maßnahmen („TOMs“) beim Auftragnehmer
**Anhang 2:** Genehmigte Unterauftragnehmer

**Anhang 1 zu Anlage 1 - Technisch-organisatorische Maßnahmen („TOMs“) beim Auftragnehmer**

*Nachfolgend aufgeführte technisch-organisatorische Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit sind derzeit beim Auftragnehmer und/oder seinen Unterauftragnehmern vorhanden:*

Technische und organisatorische Maßnahmen (TOM)
Die vorliegende Dokumentation beschreibt die vom Verantwortlichen umgesetzten technischen und organisatorischen Maßnahmen (TOM) gemäß Artikel 32 DSGVO sowie – soweit einschlägig – ergänzend nach dem Bundesdatenschutzgesetz (BDSG). Ziel ist ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten.
Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Kosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere möglicher Risiken ausgewählt und umgesetzt.
Dieses Dokument dient als Nachweis gegenüber Aufsichtsbehörden (§ 5 Abs. 2 DSGVO) und als internes Instrument zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Datenschutzmaßnahmen. Ist es Bestandteil eines Auftragsverarbeitungsvertrages (AVV), gilt es als Anlage „Technische und organisatorische Maßnahmen" und beschreibt die zum Vertragsabschluss vereinbarten Maßnahmen. Der Anwendungsbereich umfasst alle Verarbeitungsvorgänge personenbezogener Daten im Unternehmen.

## 1. Verantwortlicher

Als Verantwortlicher gilt diejenige Stelle, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Nachfolgend sind die Kontaktdaten des Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO aufgeführt:

***QLero GmbH***
*Südliche Münchner Str. 62*
*82031 Grünwald*
*Deutschland*
*E-Mail: briefkasten@qlero.de*
*Gesetzlicher Vertreter: Martin Peter Ulbricht und Moritz von Keiser*

## 2. Zuständige Datenschutzaufsichtsbehörde

Die nachfolgend genannte Datenschutzaufsichtsbehörde ist für den Verantwortlichen gemäß Art. 55 DSGVO zuständig:

***Bayerisches Landesamt für Datenschutzaufsicht** , Promenade 18 , 91522 Ansbach,*
*Telefon: +49 981 180093-0 , E-Mail: poststelle@lda.bayern.de*
*Homepage: https://www.lda.bayern.de*

## 3. Externer Datenschutzbeauftragter

Der Verantwortliche hat einen externen Datenschutzbeauftragten bestellt, der gemäß Art. 37 DSGVO wie folgt erreichbar ist:

***DATENDO GmbH**, Hohenzollernring 55, 50672 Köln, Tel. 0800 5577733,*
*E-Mail: dsgvo@datendo.de, Internet: www.datendo.de*

## 4. Gültigkeit der TOM

Die technischen und organisatorischen Maßnahmen geben den Stand vom 28.12.2025 wieder und sind in dieser Dokumentation bis einschließlich 22.11.2026 gültig. Mit Ablauf der laufenden Gültigkeitsperiode findet eine Überprüfung und gegebenenfalls eine Aktualisierung der derzeit umgesetzten und dokumentierten Maßnahmen statt.

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

### 1. Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Umgesetzte technische Maßnahmen:

**Abschließbare Türen:** Türen können gezielt verschlossen werden, um unbefugten Zutritt zu verhindern. **Sicherheitsschlösser:** hochwertige, gegen Manipulation gesicherte Schlösser für kritische Türen.
**Türen mit Knauf an der Außenseite:** verhindert das einfache Öffnen von außen, wenn kein Schlüssel vorhanden ist.
**Selbstschließende Türen mit automatischer Verriegelung:** Türen fallen nach jedem Öffnungsvorgang selbstständig ins Schloss, verriegeln sich automatisch und können nicht unbeabsichtigt offenstehen.
**Elektrische Türöffner:** fernsteuerbare Türöffnung für autorisierte Personen, z.B. durch Knopfdruck an der Zentrale.
**Code-, Transponder- oder Chipkarten für den Zutritt:** elektronische Zutrittskontrolle von Ein- und Austritten.
**Zutritt per Klingel:** Zutritt nur nach manueller Freigabe durch berechtigte Personen.
**Zutritt per Klingel mit Kameraanlage:** Zutritt nur nach Sichtprüfung und manueller Freigabe durch berechtigte Personen.
**Datenschutzkonforme Videoüberwachung der Eingänge:** Überwachung des innen liegenden Eingangsbereich unter Beachtung der Datenschutzbestimmungen.
**Verwendung einer Alarmanlage:** erkennt unbefugte Zutrittsversuche und löst akustische oder stille Alarme aus.
**Smart Locks mit App-Steuerung:** elektronische Türschlösser, die per Smartphone-App gesteuert und zeitlich begrenzt freigegeben werden können.
**Beleuchtungskonzepte zur Sicherheit:** gut ausgeleuchtete Eingangsbereiche zur besseren Kontrolle.

Umgesetzte organisatorische Maßnahmen:

**Erstellung eines Zutrittskontrollkonzepts:** Dokumentation aller Maßnahmen zur Zutrittskontrolle als Teil des Sicherheitskonzepts.
**Erstellung und Pflege eines Zutrittsberechtigungskonzepts:** Dokumentation, wer wann und wo Zutritt erhält.
**Vergabe von Zutrittsrechten nach dem „Need-to-Know"-Prinzip:** nur Personen, die es für ihre Arbeit benötigen, erhalten Zutritt.
**Rückgabe von Zutrittsmedien nach Austritt oder Funktionswechsel:** Karten, Schlüssel oder Codes müssen beim Austritt aus dem Unternehmen zurückgegeben werden.
**Verwendung einer Schlüsselliste:** Dokumentation aller ausgegebenen Schlüssel mit regelmäßiger Kontrolle.
**Notfallpläne für verlorene Schlüssel oder Zutrittsmedien:** definierte Prozesse bei Verlust von Zutrittsmedien, inklusive sofortiger Sperrung.
**Vertragliche Regelungen zur Zutrittskontrolle für externe Dienstleister:** Festlegung klarer Zutrittsregeln für externe Firmen.
**Awareness-Schulungen für Mitarbeitende zur physischen Sicherheit:** Thematisierung von Risiken wie Tailgating, Besucherumgang, Umgang mit Fremden.
**Dienstanweisung zum Verschließen der Räume:** alle Mitarbeitenden müssen sicherstellen, dass Räume nach Verlassen verschlossen sind.
**Regelmäßige Sicherheitsbegehungen:** Kontrolle, ob physische Maßnahmen tatsächlich eingehalten werden.

**Audits der Zutrittsprotokolle:** stichprobenweise Kontrolle der Protokolle auf Unregelmäßigkeiten. **Sichere Aufbewahrung von Ersatzschlüsseln:** Verwahrung in abgeschlossenen, dokumentierten Schlüsseltresoren mit Zugriffskontrolle.
**Besucherprotokollierung durch Empfangspersonal:** Erfassung der Besuchsdaten, inklusive Zweck des Besuchs.
**Besucher können das Gebäude nur betreten, wenn sie von einem der Beschäftigten in Empfang genommen und begleitet werden:** keine unbegleiteten Besucher.

## 2. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Umgesetzte technische Maßnahmen:

**Zugang nur mit Benutzerkonto und Passwort:** jede Person benötigt ein individuelles Benutzerkonto mit sicherem Passwort.
**Logins erfolgen mit Benutzername/Passwort:** Authentifizierung erfolgt über individuelle Benutzeranmeldungen.
**Mehrstufige Authentifizierung (MFA):** Zugang nur nach zusätzlicher Bestätigung, z.B. durch SMS-Code oder Authenticator-App.
**Biometrische Zugangskontrolle:** Fingerabdruck-, Gesichts- oder Iriserkennung für sichere Authentifizierung an Endgeräten.
**Logins erfolgen mit biometrischen Daten:** Fingerabdruck-, Gesichts- oder Iriserkennung als alternative Zugangsmethode.
**Automatische Zugangssperren nach Inaktivität:** Systeme sperren sich automatisch nach einer bestimmten Zeit ohne Aktivität.
**Automatische Desktopsperre bei Inaktivität:** der Bildschirm wird automatisch gesperrt, wenn keine
Aktivität erfolgt.
**Protokollierung von Zugangsaktivitäten:** alle Zugriffe auf Systeme werden dokumentiert, um eine Nachvollziehbarkeit zu gewährleisten.
**Firewall und Netzwerkzugangskontrolle:** Wir nutzen Cloud-Dienste, die entsprechend abgesichert sind
**Eine aktuelle Firewall findet Verwendung:** es wird sichergestellt, dass eine aktuelle Firewall zum Schutz der Systeme im Einsatz ist.
**Ein aktueller Spamfilter findet Verwendung:** Schutz vor unerwünschten E-Mails und Phishing- Angriffen.
**Es werden aktuelle Softwareversionen verwendet:** regelmäßige Updates zur Sicherheit und Stabilität der Systeme.
**Datenverschlüsselung bei Zugriff auf sensible Informationen:** Firmen-MacBooks sind mit aktiviertem FileVault konfiguriert.
**Verschlüsselte Datenübertragung (HTTPS/TLS):** Schutz sensibler Daten bei der Übertragung über das Netzwerk.
**Der Zugriff auf Endgeräte ist verschlüsselt:** Geräte werden durch Passwort, Fingerabdruck oder Gesichtserkennung geschützt.
**Session-Timelimits für administrative Zugänge:** automatische Beendigung von Admin-Sitzungen nach einer definierten Inaktivitätszeit.
**Analoge Daten werden in einem abgeschlossenen Schrank oder Tresor gesichert:** physische
Dokumente mit sensiblen Informationen werden sicher aufbewahrt.

Umgesetzte organisatorische Maßnahmen:

**Vergabe von Zugriffsrechten nach dem Need-to-Know-Prinzip:** nur berechtigte Personen erhalten
Zugang zu relevanten Informationen und Systemen.
**Benutzerprofile für Systeme und Programme kommen zum Einsatz:** Für alle Mitarbeitenden
jeweils individuelle Nutzerkonten

**Verfahren zur Vergabe von Lese- und Schreibrechten:** Benutzerverwaltung regelt differenzierte Zugriffsrechte.
**Strikte Trennung von administrativen und regulären Nutzerkonten:** diese sind teilweise möglich das Administratoren separate Konten für tägliche und administrative Tätigkeiten.
**Regelmäßige Überprüfung der Zugangsberechtigungen:** Zugangsrechte werden regelmäßig kontrolliert und angepasst.
**Rückgabe und Deaktivierung von Zugangsmedien nach Austritt:** sofortige Sperrung von
Benutzerkonten und Zugangskarten nach Verlassen der Organisation.
**Einführung eines rollenbasierten Berechtigungskonzepts (RBAC):** Zugriffsrechte werden systematisch über Rollen definiert.
**Regelmäßige Re-Zertifizierung von Zugriffsrechten durch Fachverantwortliche:** Fachabteilungen müssen regelmäßig prüfen und bestätigen, dass eingeräumte Rechte noch notwendig sind.
**Notfallpläne für kompromittierte Zugangsdaten:** definierte Prozesse für den Umgang mit verlorenen oder gestohlenen Zugangsdaten.
**Vertragliche Regelungen für externe Dienstleister:** klare Sicherheitsanforderungen für Dienstleister mit Zugang zu internen Systemen.
**Schulung der Mitarbeiter zur sicheren Nutzung von Zugangsdaten:** Sensibilisierung für
Passwortrichtlinien und sichere Authentifizierungsverfahren.

**Richtlinie zum verpflichtenden Einsatz einer Bildschirmsperre:** Mitarbeiter müssen eine Bildschirmsperre bei Verlassen des Arbeitsplatzes nutzen.
**Clean-Desk Vorgabe:** Arbeitsplätze müssen frei von sensiblen Dokumenten gehalten werden.
**Monitore sind stets sichtgeschützt aufgestellt:** verhindert unbefugtes Mitlesen durch Dritte.
**Richtlinie zum Datenschutz im Homeoffice/Mobile Office:** Regelungen für sicheres Arbeiten außerhalb der Betriebsstätte.
**Richtlinie zum Datenschutz:** klare Regelungen zur Einhaltung des Datenschutzes für Mitarbeitende.
**Richtlinie zum Einsatz externer Speichermedien:** Vorgaben zur Nutzung externer Speichermedien (z.B. USB-Sticks) im Unternehmen.
**Besondere Überwachung von Zugriffsversuchen auf kritische Systeme:** ungewöhnliche oder verdächtige Zugriffe werden protokolliert und überprüft.
**Verfahren zur Eskalation bei unbefugtem Zugriffsversuch:** definierter Prozess bei erkannten oder vermuteten unbefugten Zugriffen.
**Abläufe für temporäre Benutzerkonten (z.B. für Praktikanten, Auditoren):** zeitlich begrenzte Zugänge mit Ablaufdatum und eingeschränkten Rechten.

## 3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und die gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

<u>Umgesetzte technische Maßnahmen:</u>

**Vergabe von Benutzerrollen und Berechtigungen:** Zugriffsrechte werden anhand definierter Benutzerrollen vergeben.
**Zugriff nach dem „Need-to-Know"-Prinzip:** Mitarbeiter erhalten nur Zugriff auf Systeme und Daten, die für ihre Arbeit notwendig sind.
**Mehrstufige Authentifizierung (MFA):** Zusätzliche Sicherheitsstufe für den Zugriff auf kritische Systeme.
**Passwortschutz für administrative Funktionen:** Administrationsrechte erfordern gesonderte Authentifizierung.

**Automatische Sitzungsablaufzeiten:** Automatische Abmeldung von inaktiven Sitzungen zur Sicherheitserhöhung.
**Protokollierung und Monitoring von Zugriffsversuchen:** Protokollierung und Monitoring von Zugriffsversuchen haben wir nicht bei allen Systemen. Bei kritischen Cloud-Diensten ist dies jedoch implementiert.
**Temporäre Zugangsberechtigungen für bestimmte Aufgaben:** Zeitlich begrenzte Zugangsrechte für bestimmte Tätigkeiten werden Händisch sichergestellt
**Single Sign-On (SSO) für autorisierte Systeme:** Vereinfachter Zugang für Benutzer mit zentraler Authentifizierung.
**Restriktive Firewall-Regeln für Systemzugriffe:** Netzwerkzugriffe werden durch Firewalls auf autorisierte Systeme beschränkt.
**Verschlüsselte Datenübertragung und Zugriffsschutz (TLS/SSL):** Schutz der übertragenen Daten durch moderne Verschlüsselungstechnologien.
**Zugangskontrolle über biometrische Merkmale:** Fingerabdruck- oder Gesichtserkennung für hochsensible Bereiche.
**Datenträger werden verschlüsselt:** Sensible Daten auf externen und internen Speichern sind verschlüsselt.
**Nicht mehr benötigte Datenträger werden physisch gelöscht:** Datenvernichtung durch zertifizierte Methoden wie Schreddern oder Entmagnetisieren.
**Sicherungsdatenträger werden außerhalb des Unternehmens aufbewahrt:** Backups werden an einem externen, sicheren Standort gelagert.
**Datenträger werden sicher aufbewahrt (z. B. verschließbare Schränke):** Physische Speichermedien werden gegen unbefugten Zugriff gesichert.

<u>Umgesetzte organisatorische Maßnahmen:</u>
**Regelmäßige Überprüfung der Berechtigungen:** Berechtigungen werden regelmäßig kontrolliert und bei Bedarf angepasst.

**Dokumentation von Berechtigungsvergabe und -änderungen:** Alle Änderungen an Benutzerrechten werden nachvollziehbar dokumentiert.
**Rollenbasiertes Berechtigungsmanagement:** Mitarbeiter erhalten klar definierte Rollen mit spezifischen Zugriffsrechten.
**Vergabe von administrativen Rechten nur nach Freigabe:** Administrationsrechte werden nur nach schriftlicher Genehmigung vergeben.
**Rücknahme von Zugriffsrechten nach Funktionswechsel oder Austritt:** Ehemalige Mitarbeiter oder Mitarbeiter mit geänderter Rolle verlieren ungenutzte Rechte.
**Mitarbeiterschulungen zur sicheren Nutzung von Zugriffsrechten:** Regelmäßige Schulungen zu Datenschutz und Zugriffskontrolle.
**Einsatz einer Zugriffskontrollrichtlinie:** Definition und Umsetzung klarer Regeln zur Zugriffskontrolle.
**Einschränkung der Administratorrechte auf wenige, geschulte Personen:** Administrative Konten werden nur an ausgewählte Mitarbeiter vergeben.
**Benutzerrechte werden durch Administratoren anhand eines Rollen- und Berechtigungskonzepts vergeben:** Zugriffsrechte werden strukturiert und nachvollziehbar verwaltet.
**Für die Nutzung von PCs durch mehrere Beschäftigte bestehen individuelle Benutzerkonten:** Jeder Nutzer erhält ein eigenes, geschütztes Konto.
**Es gibt eine Richtlinie zum Umgang mit Datenträgern:** Definierte Regeln zur sicheren Nutzung und Lagerung von Speichermedien.
**Es besteht eine Richtlinie zur sicheren Datenträgervernichtung:** Verpflichtende Maßnahmen für die sichere Vernichtung von Datenträgern.
**Verwendung von Aktenvernichtern:** Papierunterlagen mit sensiblen Daten werden sicher entsorgt.
**Verwendung von Datenträgervernichtern:** Alte Speichermedien werden mechanisch oder elektronisch zerstört.
**Die Anzahl der Administratoren mit vollem Zugriff wird minimal gehalten:** Reduzierung von Sicherheitsrisiken durch begrenzte Administratorenanzahl.
**Notfallprozesse für unbefugten Zugriff:** Bei verdacht wird sofort der Account gesperrt

und in der GF wird darüber gesprochen und über Maßnahmen gesprochen und eingeleitet

**Deaktivierung von Zugangsdaten nach festgelegtem Zeitraum:** Regelmäßige Bereinigung nicht genutzter Konten zur Minimierung von Risiken.

**Sensibilisierung für Social-Engineering-Angriffe:** Schulungen zur Erkennung und Abwehr von Manipulationsversuchen.

**Strikte Kontrolle von Drittanbietern mit Zugriff auf Unternehmenssysteme:** Externe Dienstleister erhalten nur notwendige, befristete Zugriffsrechte.

**Vergabe von Schreib- und Leserechten je nach Aufgabengebiet:** Individuelle Rechtevergabe zur Vermeidung unnötiger Zugriffsrechte.

## 4. Trennungskontrolle

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

Umgesetzte technische Maßnahmen:

- **Trennung anhand der Ordnerstrukturen einer Festplatte:** Daten unterschiedlicher Verarbeitungszwecke werden durch getrennte Verzeichnisse organisiert.
- **Trennung von Produktiv- und Testumgebung:** Produktiv- und Testsysteme werden physisch oder logisch voneinander getrennt, um Datenverfälschungen zu vermeiden.
- **Physikalische Trennung der Systeme, Datenbanken und Datenträger:** Daten, die zu unterschiedlichen Zwecken verarbeitet werden, werden auf separaten Servern, Datenbanken oder Datenträgern gespeichert.
- **Steuerung der Verarbeitung anhand eines Berechtigungskonzepts:** Nur berechtigte Personen erhalten Zugriff auf bestimmte Datensätze oder Verarbeitungssysteme.
- **Festlegung von Datenbankzugriffsrechten:** Zugriffsrechte werden differenziert nach Benutzergruppen und Verarbeitungszweck vergeben.
- **Trennung von Zugriffsrechten je nach Datenkategorie:** Zugriffe auf personenbezogene Daten sind von Zugriffen auf sonstige nicht-personenbezogene Daten strikt getrennt.
- **Logische Trennung innerhalb von Datenbanken:** Datenbanktabellen enthalten nur zweckgebundene Informationen, um eine Vermischung zu vermeiden.
- **Steuerung der Verarbeitung durch jeweils angepasste Datenbankzugriffsrechte:** Jede Datenbank hat spezifische Zugriffsbeschränkungen, um eine ungewollte Vermischung der Daten zu

  verhindern.
- **Separate Verschlüsselung für unterschiedliche Datentypen:** Datenverschlüsselung erfolgt nach ihrem Zweck mit unterschiedlichen Schlüsseln.
- **Einsatz mandantenfähiger Systeme:** Systeme ermöglichen es, Daten mehrerer Organisationseinheiten (z.B. Kunden) technisch voneinander zu trennen (z.B. durch Mandantenstrukturen in Cloud-Anwendungen).

Umgesetzte organisatorische Maßnahmen:

- **Regelmäßige Überprüfung der Trennungsmaßnahmen:** Interne Audits stellen sicher, dass die Datentrennung gewahrt bleibt.
- **Löschkonzept für nicht mehr benötigte Daten unterschiedlicher Zwecke:** Regelmäßige Löschung oder Anonymisierung von Daten nach Ablauf der Speicherfrist.
- **Verfahrensanweisungen zur getrennten Verarbeitung:** Es ist festgelegt, welche Systeme oder Prozesse für welche Datenzwecke verwendet werden dürfen.
- **Schulung der Mitarbeitenden zur Trennung personenbezogener Daten:** Mitarbeitende werden für die Bedeutung und Umsetzung der Trennung sensibilisiert.

**5. Pseudonymisierung**

Maßnahmen, die gewährleisten, dass 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, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden und auch nicht zugewiesen werden können.

Umgesetzte technische Maßnahmen: ---

Umgesetzte organisatorische Maßnahmen: --

**11.** Integrität (Art. 32 Abs. 1 lit. b DSGVO)

**1.** Weitergabekontrolle

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

Umgesetzte technische Maßnahmen:

- **Zugriffsprotokollierung bei Cloud-Freigaben:** Dateiabrufe über geteilte Cloud-Plattformen werden automatisch protokolliert.
- **Nutzung von Signaturverfahren:** Elektronische Dokumente und Verträge werden mit Signaturverfahren gesichert.
- **Sicherung der Übermittlung anhand eines Verfahrensverzeichnisses:** Datenweitergaben erfolgen nach festgelegten, dokumentierten Verfahren.

Umgesetzte organisatorische Maßnahmen:

- **Weitergabe erfolgt nur an berechtigte Empfänger gemäß Datenschutzvorgaben:** Die Weitergabe erfolgt nur an befugte Personen oder Organisationen, die nachweislich zur Verarbeitung berechtigt sind.
- **Einhaltung gesetzlicher und vertraglicher Vorschriften zur Weitergabe:** Alle Datenweitergaben erfolgen unter Beachtung der gesetzlichen Datenschutzanforderungen und vertraglichen Regelungen.
- **Die Empfänger von Daten werden dokumentiert und kontrolliert:** Alle Empfänger personenbezogener oder sensibler Daten werden registriert und regelmäßig überprüft.
- **Der Zeitraum der Überlassung der Daten wird protokolliert:** Die Dauer der Datenweitergabe wird dokumentiert, um eine fristgerechte Rückführung oder Löschung sicherzustellen.
- **Vertraulichkeitsvereinbarungen bei interner Weitergabe:** Mitarbeitende, die intern sensible Daten weiterleiten oder empfangen, sind vertraglich zur Vertraulichkeit verpflichtet.

- **Verpflichtungserklärungen oder NDA für Externe vor der Datenweitergabe:** Externe Dienstleister oder Empfänger erhalten Zugang zu personenbezogenen Daten nur nach Unterzeichnung einer Verschwiegenheitserklärung oder eines Auftragsverarbeitungsvertrags.

**2.** Eingabekontrolle

Maßnahmen, die es erlauben, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind und ob diese den Ursprungsdaten entsprechen.

Umgesetzte technische Maßnahmen:

- **Die Eingabe, Veränderung und Löschung von Daten werden technisch protokolliert:** Alle Änderungen in Clickup, Sharepoint und Onedrive werden automatisch protokolliert, um eine lückenlose Nachverfolgbarkeit sicherzustellen.
- **Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen:** Jede Dateneingabe, -änderung oder -löschung ist mit einem spezifischen Benutzerkonto verknüpft.
- **Einsatz von Logging-Mechanismen:** Systeme speichern sämtliche Eingaben, Änderungen und Löschungen in Audit-Logs.
- **Zeitstempel für jede Eingabe, Änderung oder Löschung:** Jede Änderung wird mit einem exakten Zeitstempel versehen, um eine vollständige Nachvollziehbarkeit zu gewährleisten.
- **Einsatz von Versionierungssystemen für Dateneingaben:** Veränderte oder gelöschte Daten werden in Versionierungsprotokollen gespeichert, um eine Wiederherstellung zu ermöglichen.
- **Vergabe von Zugriffsberechtigungen:** Nutzer erhalten nur die Rechte zur Dateneingabe oder -änderung, die für ihre Aufgaben erforderlich sind.
- **Technische Schutzmaßnahmen gegen unautorisierte Datenveränderungen:** Zugriffsrechte und Mechanismen wie Mehrfaktor-Authentifizierung verhindern unbefugte Änderungen.
- **Automatische Validierung der eingegebenen Daten:** Eingaben werden automatisch auf Plausibilität und Vollständigkeit geprüft.
- **Sichtschutzmasken für Eingabefelder mit sensiblen Daten:** In Benutzeroberflächen werden sensible Eingaben wie Passwörter automatisch verdeckt dargestellt.
- **Konfigurierbare Rollen für Eingabeprozesse in Workflows:** Systeme erlauben eine granulare Zuweisung, welche Nutzer welche Eingabefelder und Masken bearbeiten dürfen.

Umgesetzte organisatorische Maßnahmen:

- **Klare Dokumentation von Berechtigungsvergaben:** Alle Zugriffsrechte auf Dateneingabe und - veränderung werden dokumentiert und regelmäßig überprüft.
- **Vier-Augen-Prinzip für kritische Dateneingaben:** Sensible oder besonders relevante Eingaben werden von einer zweiten Person überprüft.
- **Einhaltung gesetzlicher Vorschriften zur Dateneingabe und -löschung:** Alle Eingabe- und Löschprozesse entsprechen den Datenschutzvorgaben der DSGVO und weiteren relevanten Gesetzen.
- **Dokumentierte Freigabeprozesse für strukturrelevante Dateneingaben:** Für Daten mit systemischen Auswirkungen (z.B. in CRM oder ERP) existieren dokumentierte Freigaben.

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

### 1. Verfügbarkeitskontrolle

Maßnahmen zur Wahrung der Verfügbarkeit stellen sicher, dass verarbeitete personenbezogene Daten auch bei technischen Störungen, Ausfällen oder sonstigen Zwischenfällen weiterhin zugänglich sind und der Geschäftsbetrieb ohne wesentliche Einschränkungen fortgeführt werden kann.

Umgesetzte technische Maßnahmen: ---

Umgesetzte organisatorische Maßnahmen:

- **Notfallplan für IT-Ausfälle:** Vorgehensweise bei Ausfällen ist schriftlich dokumentiert und abrufbar.
- **Zuständigkeiten für IT-Notfälle klar definiert:** Im Ernstfall sind Aufgaben und Ansprechpartner eindeutig geregelt.

- **Verfügbarkeitskontrollrichtlinie im IT-Sicherheitskonzept verankert:** Die Grundsätze der Verfügbarkeitskontrolle sind Bestandteil eines übergeordneten Sicherheitskonzepts.
- **Einsatz eines nach ISO 27001 zertifizierten Hosting-Unternehmens:** Der eingesetzte Hostingpartner verfügt über ein zertifiziertes Informationssicherheits-Managementsystem (ISMS).
- **Einsatz von Rechenzentren mit hohen Sicherheitsstandards:** Unser Hosting-Unternehmen schützt seine Server durch mehrstufige physische und technische Sicherheitsmaßnahmen.

**2.** Wiederherstellbarkeit

Maßnahmen zur Wiederherstellbarkeit gewährleisten, dass nach einem Verlust oder einer Beeinträchtigung personenbezogener Daten deren Verfügbarkeit zeitnah und in angemessener Qualität wiederhergestellt wird, um einen ordnungsgemäßen Betrieb sicherzustellen.

Umgesetzte technische Maßnahmen:

- **Datensicherungskonzept vorhanden:** Definierte Strategie zur regelmäßigen Sicherung und Wiederherstellung von Daten.
- **Backup-Konzept:** Systematische Planung und Durchführung regelmäßiger Datensicherungen.
- **Speicherung von Backups an einem externen Ort:** Sicherungskopien werden an einem räumlich getrennten, sicheren Standort aufbewahrt.
- **Automatisierte Backup-Prozesse mit Versionierung:** Backups werden regelmäßig erstellt und mit Zeitstempeln versehen.
- **Georedundante Backup-Speicherung:** Verteilung von Backups auf verschiedene geografische Standorte zur Absicherung gegen Standortausfälle.
- **Backup-Monitoring-Systeme:** wird an unseren Diesntleistern mittels AVV durchgereicht für die Automatisierte Überwachung und Alarmierung bei fehlgeschlagenen oder unvollständigen Backups.
- **Trennung von Backup- und Live-Systemen (Air Gap):** Offline-Backups oder netzwerkgetrennte Speicher zur Abwehr von Schadsoftware.

Umgesetzte organisatorische Maßnahmen:

- **Notfallplan/Wiederanlaufplan:** Detaillierter Plan zur schnellen Wiederherstellung der IT-Systeme im Störungsfall.
- **Regelmäßige Überprüfung der Backup-Prozesse:** Wir durch unseren Cloudanbieter Kontinuierliche Überwachung und Verbesserung der Datensicherungsstrategien.
- **Schulungen für IT-Personal zur Wiederherstellung von Systemen:** Mitarbeitende werden in der schnellen und sicheren Wiederherstellung geschult.
- **Dokumentation der Backup- und Wiederherstellungsverfahren:** muss an unserem Cloudanbieter durchgereicht werden das alle Prozesse nachvollziehbar dokumentiert und werden regelmäßig aktualisiert.
- **Vertragliche Regelungen mit IT-Dienstleistern zur schnellen Wiederherstellung:** Externe Partner garantieren bestimmte Reaktionszeiten im Notfall.
- **Einhaltung gesetzlicher Anforderungen zur Datensicherung:** Backups und Wiederherstellungsmethoden entsprechen DSGVO und BDSG.
- **Verantwortlichkeiten für Backup und Wiederherstellung klar geregelt:** Zuständigkeiten und Vertretungen sind schriftlich definiert.
- **Zeitpläne und Wiederanlaufprioritäten im Notfallplan definiert:** Kritische Systeme werden zuerst wiederhergestellt – abgestuft nach Priorität.
- **Regelmäßige Schulungen zu Ransomware-Schutz und Backup-Strategien:** Prävention und Reaktionsfähigkeit werden durch Weiterbildung gestärkt.
- **Protokollierung und Nachvollziehbarkeit jeder Wiederherstellung:** Die ist in der AVV und Toms übersicht unser Cloudanbieter geregelt das jeder Wiederherstellungsvorgang wird mit Uhrzeit, Dateninhalt und Akteur dokumentiert.

## **IV.** Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; ergänzend Art. 25 und Art. 28 DSGVO)

### **1.** Datenschutz durch Technik

Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, also Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Umgesetzte technische Maßnahmen:

- **Minimaldatenerhebung:** Es werden nicht mehr Daten erhoben, als für den jeweiligen Zweck erforderlich ist (Datensparsamkeit).
- **Einfache Ausübung eines Widerspruchs zu einer Einwilligung durch technische Maßnahmen:** Nutzer können ihre Einwilligung einfach über digitale Schnittstellen widerrufen, z. B. über Datenschutzeinstellungen oder ein Benutzerkonto.
- **Anonymisierung und Pseudonymisierung personenbezogener Daten:** Personenbezogene Daten werden, wo immer möglich, anonymisiert oder pseudonymisiert verarbeitet.
- **Automatische Löschung personenbezogener Daten nach Ablauf der Speicherfrist:** Daten werden nach definierten Zeiträumen automatisiert gelöscht, um eine unnötige Speicherung zu vermeiden.
- **Technische Maßnahmen zur Beschränkung der Zugänglichkeit:** Daten sind durch technische Voreinstellungen nur für berechtigte Personen zugänglich (z. B. durch rollenbasierte Zugriffsrechte).
- **Standardmäßig aktivierte Datenschutzeinstellungen:** Voreinstellungen in Systemen und Anwendungen sind datenschutzfreundlich, sodass Nutzer aktiv in weitergehende Datennutzungen einwilligen müssen.
- **Technische Voreinstellung zur Beschränkung der Speicherdauer:** Daten werden anhand vordefinierter Speicherfristen teilweise automatisch gelöscht oder archiviert.
- **Zwangsanonymisierung sensibler Daten in Test- und Entwicklungsumgebungen:** In nicht- produktiven Umgebungen werden personenbezogene Daten durch Dummy-Daten ersetzt.
- **Standardmäßige Deaktivierung nicht notwendiger Funktionen (Opt-In):** Funktionen wie Standortfreigabe, Kamera oder Mikrofon sind standardmäßig deaktiviert und müssen bewusst aktiviert werden.
- **Technische Voreinstellungen zur Minimierung bei Formularfeldern:** Nur erforderliche Felder sind verpflichtend; weitere Angaben sind optional.

Umgesetzte organisatorische Maßnahmen:

- **Datenschutzfreundliche Voreinstellungen als Standard:** Systeme und Anwendungen sind standardmäßig so konfiguriert, dass nur die notwendigsten Daten verarbeitet werden.
- **Regelmäßige Datenschutzprüfungen und Audits:** Systeme werden regelmäßig auf Datenschutzkonformität geprüft und notwendige Anpassungen vorgenommen.
- **Dokumentation von Datenschutzmaßnahmen in technischen Konzepten:** Alle datenschutzrelevanten Maßnahmen sind in IT- und Datenschutzkonzepten dokumentiert.
- **Sensibilisierung und Schulung von Mitarbeitenden zu Datenschutzmaßnahmen:** Mitarbeitende werden regelmäßig zum Prinzip der Datensparsamkeit und zu datenschutzfreundlichen Einstellungen geschult.
- **Verpflichtung von Drittanbietern zur Umsetzung datenschutzfreundlicher Voreinstellungen:** Externe Dienstleister müssen sicherstellen, dass ihre Systeme datenschutzkonform voreingestellt sind.
- **Berücksichtigung von Datenschutzprinzipien bei der Entwicklung neuer IT-Systeme:** Bereits bei der Konzeption und Implementierung neuer Anwendungen werden datenschutzfreundliche Voreinstellungen integriert.
- **Regelmäßige Kontrolle der Zugriffsbeschränkungen:** Überprüfung, ob nur berechtigte Personen auf personenbezogene Daten zugreifen können.

- **Review-Prozess vor dem Rollout neuer Anwendungen:** Vor der Einführung neuer IT-Systeme wird geprüft, ob Datenschutzprinzipien wie Datensparsamkeit und Zweckbindung technisch umgesetzt sind.

**2.** Auftragskontrolle als Auftraggeber

Maßnahmen, die sicherstellen, dass ein beauftragter Auftragsverarbeiter personenbezogene Daten ausschließlich entsprechend den dokumentierten Weisungen des Auftraggebers verarbeitet und diese Weisungen unverzüglich umsetzt.

Umgesetzte technische Maßnahmen:

- **Verschlüsselte Übermittlung von Daten an Auftragsverarbeiter:** Der Auftraggeber stellt sicher, dass die Datenübertragung nur über verschlüsselte Kanäle (z. B. SFTP, TLS, VPN) erfolgt.
- **Technische Zugriffsbeschränkungen für Auftragsverarbeiter:** Der Auftraggeber definiert und kontrolliert, dass der Auftragsverarbeiter nur Zugriff auf notwendige Daten erhält (Least-Privilege-Prinzip).
- **Protokollierung der Datenverarbeitung durch Auftragsverarbeiter:** Der Auftraggeber stellt sicher, dass der Auftragsverarbeiter die Verarbeitung und Zugriffe auf personenbezogene Daten protokolliert.
- **Technische Maßnahmen zur Löschung und Vernichtung von Daten nach Auftragsende:** Der Auftraggeber definiert vertraglich und prüft, dass personenbezogene Daten nach Beendigung des Auftrags sicher gelöscht oder vernichtet werden.
- **Regelmäßige Sicherheitsüberprüfungen der IT-Systeme der Auftragsverarbeiter:** Der Auftraggeber behält sich vor, Sicherheitsprüfungen oder Audits durchzuführen.

Umgesetzte organisatorische Maßnahmen:

- **Sorgfältige Auswahl von Auftragsverarbeitern:** Der Auftraggeber prüft vor der Beauftragung, ob der Auftragsverarbeiter geeignete Datenschutzmaßnahmen implementiert hat.
- **Abschluss eines Auftragsverarbeitungsvertrags (AVV):** Der Auftraggeber schließt mit dem Auftragnehmer einen AVV gemäß DSGVO ab.
- **Vereinbarung von Kontrollrechten:** Der Auftraggeber behält sich das Recht vor, Datenschutzprüfungen oder Audits beim Auftragnehmer durchzuführen.
- **Tatsächliche Vor-Ort-Kontrolle der Auftragsausführung:** Bei besonders sensiblen Verarbeitungen führt der Auftraggeber Vor-Ort-Kontrollen durch.
- **Sicherstellung der Vernichtung/Löschung von Daten nach Auftragsbeendigung:** Der Auftraggeber stellt sicher, dass die vereinbarten Maßnahmen zur Datenlöschung durch den Auftragnehmer umgesetzt werden.
- **Dokumentation der Datenverarbeitung durch den Auftragsverarbeiter:** Der Auftraggeber verpflichtet den Auftragnehmer, sämtliche relevanten Verarbeitungsvorgänge zu dokumentieren.
- **Verpflichtung des Auftragsverarbeiters zur Benennung eines Datenschutzbeauftragten (sofern erforderlich):** Der Auftraggeber stellt sicher, dass ein zuständiger Ansprechpartner beim Auftragsverarbeiter vorhanden und erreichbar ist.
- **Klare Prozesse bei Datenschutzvorfällen beim Auftragsverarbeiter:** Der Auftraggeber verpflichtet den Auftragsverarbeiter, Datenschutzverletzungen unverzüglich zu melden, inklusive klar definierter Fristen und Eskalationsmechanismen.

**3.** Auftragskontrolle als Auftragnehmer

Maßnahmen, die gewährleisten, dass personenbezogene Daten im Rahmen einer Auftragsverarbeitung nur gemäß den vom Auftraggeber erteilten Weisungen verarbeitet werden. Eingehende Weisungen werden dokumentiert, auf Umsetzbarkeit geprüft und unverzüglich umgesetzt.

Umgesetzte technische Maßnahmen:

- **Zugangskontrollen für Systeme mit Auftragsdaten:** Der Auftragnehmer setzt technische Schutzmaßnahmen wie Passwörter, Zwei-Faktor-Authentifizierung oder rollenbasierte Zugriffsrechte ein, um den Zugriff auf personenbezogene Daten auf autorisierte Nutzer zu beschränken.
- **Sicherstellung der sicheren Datenübertragung:** Datenübertragungen zwischen dem Auftragnehmer und Dritten (z.B. dem Auftraggeber oder Unterauftragnehmern) erfolgen ausschließlich über gesicherte, verschlüsselte Übertragungswege wie TLS oder VPN.
- **Technische Maßnahmen zur Löschung und Vernichtung von Daten nach Auftragsende:** Der Auftragnehmer implementiert datenschutzkonforme Verfahren zur sicheren und vollständigen Löschung oder Vernichtung der personenbezogenen Daten nach Abschluss der vertraglich vereinbarten Verarbeitung.
- **Protokollierung von Verarbeitungsvorgängen:** Alle relevanten Datenverarbeitungstätigkeiten werden automatisch und nachvollziehbar protokolliert (z.B. Zugriffe, Änderungen, Exporte), um eine lückenlose Kontrolle und Nachverfolgbarkeit zu gewährleisten.
- **Mandantenfähigkeit der Systeme:** IT-Systeme des Auftragnehmers trennen Daten verschiedener Auftraggeber logisch oder physisch, sodass keine ungewollte Vermischung der Verarbeitung stattfinden kann.
- **Technische Beschränkung von Export- und Downloadfunktionen:** Datenexporte sind nur für berechtigte Benutzer möglich, können zusätzlich freigabepflichtig sein oder werden protokolliert.
- **Monitoring-Systeme zur Erkennung unzulässiger Datenzugriffe:** Der Auftragnehmer betreibt ein technisches Monitoring, das ungewöhnliche oder unzulässige Datenzugriffe erkennt und automatische Sicherheitsmechanismen auslöst (z.B. Alarmierung, Sperrung, Logging).

Umgesetzte organisatorische Maßnahmen:

- **Einhaltung des Auftragsverarbeitungsvertrags:** Der Auftragnehmer richtet alle internen Prozesse so aus, dass die Vorgaben aus dem abgeschlossenen Auftragsverarbeitungsvertrag (AVV) vollständig erfüllt werden.
- **Schulungen der Mitarbeitenden zum Datenschutz:** Alle mit personenbezogenen Daten befassten Mitarbeitenden erhalten regelmäßig Datenschutzschulungen, insbesondere zum Umgang mit Auftragsdaten, zu Sicherheitsanforderungen und zur Meldung von Vorfällen.
- **Mitarbeitende werden zur Vertraulichkeit verpflichtet:** Der Auftragnehmer stellt sicher, dass alle Mitarbeitenden eine schriftliche Vertraulichkeitserklärung unterzeichnet haben, bevor sie Zugriff auf personenbezogene Daten erhalten.
- **Sicherstellung der Nutzung sicherer IT-Systeme:** Der Auftragnehmer überprüft regelmäßig, ob die eingesetzten Hard- und Softwaresysteme aktuellen Sicherheitsstandards entsprechen und nur autorisierten Zugriff zulassen.
- **Regelmäßige interne Überprüfung der Datenschutzmaßnahmen:** Interne Audits oder Selbstprüfungen stellen sicher, dass Datenschutzvorgaben fortlaufend eingehalten werden und Prozesse ggf. angepasst werden.
- **Dokumentation aller Maßnahmen zur Einhaltung des Datenschutzes:** Sämtliche umgesetzten technischen und organisatorischen Maßnahmen werden nachvollziehbar dokumentiert, um auf Anfrage des Auftraggebers oder der Aufsichtsbehörde nachgewiesen werden zu können.
- **Benennung eines Ansprechpartners oder Datenschutzbeauftragten:** Der Auftragnehmer benennt eine verantwortliche Person (intern oder extern), die für die Umsetzung der Datenschutzvorgaben zuständig ist und für den Auftraggeber als Ansprechpartner fungiert.
- **Interne Meldeprozesse für Datenschutzvorfälle:** Es bestehen verbindliche Prozesse, wie Mitarbeitende Datenschutzverletzungen melden müssen. So wird eine unverzügliche Information des Auftraggebers gemäß Art. 33 DSGVO sichergestellt.
- **Richtlinie zum Umgang mit Supportzugriffen auf Auftragsdaten:** Supportleistungen, die Zugriff auf personenbezogene Daten erfordern, erfolgen nur mit vorheriger Genehmigung und unter Dokumentation der jeweiligen Maßnahmen.

- **Organisatorische Trennung von Verarbeitungen für unterschiedliche Auftraggeber:** Die Auftragsverarbeitung erfolgt strikt nach Mandantenzuordnung. Prozesse, Systeme und Dokumentation gewährleisten eine saubere Trennung von Aufträgen und Datensätzen unterschiedlicher Kunden.

## V. Datenschutz-Management

Der Verantwortliche hat ein umfassendes Datenschutz-Managementsystem etabliert, das über die rein technischen und organisatorischen Einzelmaßnahmen hinausgeht. Ziel ist es, den Datenschutz ganzheit-lich in die Organisationsprozesse zu integrieren und kontinuierlich zu verbessern. Kernbestandteile dieses Systems sind:

- Verbindliche Leitlinien und Richtlinien: Alle datenschutzrechtlich relevanten Prozesse sind in einem Datenschutz-Management-Handbuch dokumentiert. Dieses Handbuch dient als verbindliche Grundlage für Beschäftigte und sonstige Person innerhalb der Organisation.
- Regelmäßige Schulungen und Sensibilisierung: Mitarbeitende werden fortlaufend zu datenschutz- rechtlichen Anforderungen, technischen Maßnahmen sowie zu einem verantwortungsvollen Umgang mit personenbezogenen Daten geschult.
- Kontinuierliche Überwachung und Aktualisierung: Die Datenschutzmaßnahmen werden regelmäßig überprüft und an neue rechtliche, organisatorische und technische Entwicklungen angepasst.
- Einbindung des Datenschutzbeauftragten: Der externe Datenschutzbeauftragte begleitet sämtliche Prozesse beratend und überprüfend, um die Einhaltung der gesetzlichen Anforderungen sicherzustellen.

Die Einzelheiten zu diesen Maßnahmen ergeben sich aus dem Datenschutz-Management-Handbuch, welches die hier dargestellten TOM ergänzt und eine umfassende Übersicht über die organisatorischen Abläufe, Zuständigkeiten und Prozesse im Datenschutz bietet.

**Anhang 2 zu Anlage 1 - Genehmigte Unterauftragnehmer**

Nachfolgend werden die im Rahmen der Auftragsverarbeitung eingesetzten Subunternehmer gemäß Art. 28 DSGVO aufgeführt. Der Auftraggeber genehmigt zum Zeitpunkt des Abschluss des Hauptvertrags den Einsatz der nachfolgend aufgeführten Unterauftragnehmer des Auftragnehmers:

| **Name des Unterauftragnehmers** | **Anschrift/Land** | **Leistungsinhalt** | **Angaben zu geeigneten Garantien für Datenübermittlung ins Drittland** |
|---|---|---|---|
| Bare.ID GmbH | Kirchgasse 6, 65185 Wiesbaden | Identity & Access Management (IAM), Single-Sign-on (SSO) für Unternehmen | Nicht erforderlich |
| IONOS SE | Elgendorfer Str. 57, 56410 Montabaur | Hosting/Cloud, Domains, E-Mail, Infrastruktur | Nicht erforderlich |
| Sendinblue GmbH (Brevo) | Köpenicker Str. 126, 10179 Berlin | E-Mail-Marketing, Transaktionsmails, Kundenkommunikation, CRM & Marketing-Automation | Nicht erforderlich |
| Stripe Payments Europe Ltd. | 1 Grand Canal Street Lower, Grand Canal Dock, Dublin D02 H210, Irland | Zahlungsdienst zur Zahlungsabwicklung, Payment Gateway, Betrugsprävention | Nicht erforderlich |
| Qutee GmbH | Gerichtsstraße 2, 65185 Wiesbaden | Telefonie-Anbieter für KI-gestützten Kundensupport | Nicht erforderlich |
| TBA | TBA | Chat mit KI-gestützten Kunden und Produkt Support | Nicht erforderlich |

mAikit.AI

**Anlage 2 – Vereinbarung zum Cloud-Switching nach Data Act**

## 1. Erfüllung der Informationspflichten

1.1. Der Kunde erhält vom Anbieter im **Anhang** die folgenden Informationen nach Art. 25, Art. 26, Art. 28 und 29 Data Act:

1.1.2. zu den Standard-Servicegebühren und gegebenenfalls zu den Strafen für eine vorzeitige Beendigung;
1.1.3. zu den Wechselentgelten;
1.1.4. eine erschöpfende Auflistung der Kategorien von Daten und digitalen Vermögenswerten, die exportiert werden können;
1.1.5. eine erschöpfende Auflistung der Datenkategorien, die für den internen Betrieb des Datenverarbeitungsdienstes des Anbieters spezifisch sind und von der Verpflichtung zum Datenexport ausgenommen sind, wenn die Gefahr einer Verletzung der Geschäftsgeheimnisse des Anbieters besteht.
1.1.6. Informationen zu den Verfahren für den Wechsel vom Datenverarbeitungsdienst, die maschinenlesbaren Datenformate, in denen die Nutzerdaten exportiert werden können, die Instrumente für den Datenexport, einschließlich offener Schnittstellen, Informationen zur Kompatibilität mit harmonisierten Normen oder gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen, Informationen über technische Beschränkungen und Einschränkungen, die sich auf den Vollzug des Wechsels auswirken und die geschätzte Zeit, die erforderlich ist, um den Wechsel zu vollziehen.
1.1.7. Die Webseite des Online-Registers des Anbieters mit Datenstrukturen und -formaten, relevanten Standards und offenen Interoperabilitätsspezifikationen, in denen die 1.1.4 genannten exportierbaren Daten verfügbar sind.
1.1.8. Die Webseite des Anbieters mit Informationen in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld.
1.1.9. Gegebenenfalls Informationen über Datenverarbeitungsdienste, durch die der Wechsel sehr kompliziert oder kostspielig wird oder ohne nennenswerte Eingriffe in die Daten, digitalen Vermögenswerte oder die Dienstarchitektur unmöglich ist.

## 2. Einleitung des Wechselvorgangs

2.1. Der Kunde hat dem Anbieter eine Wechselmitteilung mindestens in Textform zukommen zu lassen, mit der er den Wechsel einleitet.
2.2. In einer solchen Wechselmitteilung hat der Kunde mitzuteilen, ob er beabsichtigt:
2.2.1. zu einem anderen Anbieter von Datenverarbeitungsdiensten zu wechseln. In diesem Fall sollte der Kunde die erforderlichen Angaben zum Zielanbieter machen, insbesondere Name, Anschrift und Webseite;
2.2.2. zu einer lokalen IKT-Infrastruktur des Kunden zu wechseln; oder
2.2.3. nicht zu wechseln, sondern seine exportierbaren Daten und digitalen Vermögenswerte beim Anbieter zu löschen.
2.3. Der Anbieter wird dem Kunden den Erhalt der Wechselmitteilung spätestens innerhalb von 5 Werktagen auf dem gleichen Kommunikationsweg bestätigen, den der Kunde verwendet hat.

## 3. Übergangszeitraum im Fall eines Wechsels

3.1. Der verbindliche maximale Übergangzeitraum im Fall eines Wechsels beträgt 2 Monate (Kündigungsfrist nach Art. 25 Abs. 2 lit. d Data Act) und 30 Kalendertage (Übergangsfrist nach Art. 25 Abs. 2 lit. a Data Act).
3.2. Wenn der Anbieter den verbindlichen maximalen Übergangszeitraum für den Wechsel von 2 Monaten und 30 Kalendertagen aus technischen Gründen nicht einhalten kann, verpflichtet er sich:

3.2.1. den Kunden innerhalb von 14 Werktagen nach Erhalt der Kündigungsmitteilung schriftlich, einschließlich auf geeigneten elektronischen Weg, zu benachrichtigen;
3.2.2. eine alternative Übergangszeit anzugeben, die sieben 7 Monate ab Zugang der Mitteilung eines Wechsels nach 2.1. nicht überschreiten darf; und
3.2.3. die technische Unmöglichkeit angemessen zu begründen.
Der Kunde hat den Erhalt dieser Verlängerungsmitteilung innerhalb von 3 Werktagen zu bestätigen.
3.3. Der Kunde kann die Übergangszeit einmalig um einen Zeitraum verlängern, den er für seine Zwecke für angemessener hält, jedoch nicht länger als 8 Monate nach Zugang der Mitteilung eines Wechsels nach 2.1. In diesem Fall muss der Kunde den Anbieter schriftlich, auch auf elektronischem Wege, über seine Absicht bis zum Ende der ursprünglichen Übergangszeit von 2 Monaten und 30 Kalendertagen informieren und die alternative Übergangszeit angeben. Der Anbieter wird den Erhalt einer solchen Verlängerungsmitteilung innerhalb von 5 Werktagen bestätigen.

**4. Pflichten des Anbieters während des Wechselprozesses**

4.1. Der Anbieter verpflichtet sich, dem Kunden und den vom Kunden bevollmächtigten Dritten nach Beginn des Wechselprozesses und während dessen gesamten Dauer angemessene Unterstützung zu leisten, damit der Kunde innerhalb des vorgeschriebenen maximalen Übergangszeitraums (2 Monate und 30 Kalendertage) wechseln kann. Zu diesem Zweck wird der Anbieter insbesondere:
4.1.1. Fähigkeiten, angemessene Informationen (einschließlich der für den Wechsel erforderlichen Unterlagen) und technische Unterstützung bereitstellen. Werden Probleme festgestellt, analysieren der Anbieter und der Kunde in gutem Glauben die Ursachen und vereinbaren Lösungen.
4.1.2. Mit der gebotenen Sorgfalt handeln, um die Geschäftskontinuität aufrechtzuerhalten und die Funktionen oder Dienstleistungen gemäß der Vereinbarung weiterhin bereitzustellen.
4.1.3. Während des gesamten Wechselprozesses ein hohes Maß an Sicherheit gewährleisten, insbesondere für die Sicherheit der Daten während ihrer Übertragung.

**5. Pflichten des Kunden während des Wechselprozesses**

5.1. Der Kunde verpflichtet sich, alle angemessenen Maßnahmen zu ergreifen, um einen effektiven Wechsel zu erreichen. Der Kunde verpflichtet sich, die Verantwortung für den Import und die Implementierung von Daten und digitalen Assets in seinen eigenen Systemen oder in den Systemen des Zielanbieters zu übernehmen.
5.2. Der Kunde verpflichtet sich, die geistigen Eigentumsrechte an allen Materialien, die vom Anbieter im Rahmen des Wechsels bereitgestellt werden, sowie die Geschäftsgeheimnisse des Anbieters vertraulich zu behandeln und sicherzustellen, dass von ihm beauftragte Dritte, einschließlich des Zielanbieters dies gleichfalls tun. Für den Fall, dass der Kunde Dritten Zugang zu diesen Materialien gewähren muss, verpflichtet er sich dies nur in dem Umfang zu tun, der zur Durchführung des Wechselvorgangs bis zum Ende des maximalen verbindlichen Übergangszeitraums, einschließlich der alternativen Übergangszeit, erforderlich ist, wobei gleichzeitig die Vertraulichkeitsverpflichtungen sowie die vom Anbieter gewährten Rechte an geistigem Eigentum zu beachten sind.

**6. Datenabruf und Löschung von Daten im Fall eines Wechsels**

6.1. Im Fall eines Wechsels nach 2.2.1. oder 2.2.2. kann der Kunde seine Daten während der Datenabrufperiode von 30 Kalendertagen, die ab Ablauf des verbindlichen maximalen Übergangszeitraums (3.1.) oder des verlängerten Übergangszeitraums (3.2.) beginnt, beim Anbieter abrufen oder löschen.
6.2. Nach Ablauf der vereinbarten Datenabrufperiode nach 6.1. oder der nach Ablauf eines vereinbarten alternativen Zeitraums als der Datenabrufperiode nach 6.1. und nach erfolgreichem Abschluss des Wechselvorgangs verpflichtet sich der Anbieter, alle vom Kunden generierten

oder direkt mit dem Kunden in Verbindung stehenden exportierbaren Daten und digitalen Vermögenswerte zu löschen und dem Kunden dies zu bestätigen, mit Ausnahme der personenbezogenen exportierbaren Daten, zu deren Speicherung der Anbieter gemäß EU- oder nationalen Gesetzen verpflichtet ist.
6.3. Auch während der Datenabrufperiode hat der Anbieter für ein hohes Maß an Sicherheit zu sorgen.

**7. Beendigung des Vertrags und Folgen**

7.1. Unbeschadet der Regelungen zwischen den Parteien zur Kündigung des Vertrages, gilt im Falle der Einleitung eines Wechsels nach Ziffer 2. der Vertrag zwischen den Parteien dann als beendet, wenn eines der folgenden Ereignisse vollständig eingetreten ist:
7.1.1. Gegebenenfalls nach erfolgreichem Abschluss des Wechselvorgangs („Ereignis A“). Tritt Ereignis A vor Ablauf der vereinbarten Vertragslaufzeit ein, gelten die im Anhang festgelegten Gebühren für vorzeitige Kündigung, oder;
7.1.2. Am Ende der Kündigungsfrist von zwei Monaten, wenn der Kunde nicht wechseln, sondern seine exportierbaren Daten und digitalen Vermögenswerte bei Beendigung des Dienstes löschen möchte („Ereignis B“).
7.2. Sobald der Kunde dem Anbieter mitteilt, dass der Wechselvorgang erfolgreich abgeschlossen ist, verpflichtet sich der Anbieter, den Kunden unverzüglich über die Beendigung des Vertrags zu informieren.
Wenn der Kunde den Anbieter nicht über den erfolgreichen Wechsel oder dessen Ausbleiben informiert, der Anbieter jedoch berechtigte Gründe zu der Annahme hat, dass der Wechsel vom Kunden erfolgreich abgeschlossen wurde, kann der Anbieter dem Kunden eine Anfrage zur Bestätigung des erfolgreichen Wechsels zusenden. Wenn der Kunde den erfolgreichen Wechsel nicht innerhalb von 30 Werktagen nach dieser Anfrage bestätigt, gilt der Wechsel, als nicht erfolgreich und der Vertrag wird nicht beendet, sondern zu den bestehenden Bedingungen fortgesetzt.
7.3. Wenn der in Ziffer 7.1.1. beschriebene Wechselvorgang nicht erfolgreich abgeschlossen werden kann, müssen die Parteien in gutem Glauben zusammenarbeiten, um das Problem zu identifizieren und zu lösen, damit der Wechselvorgang verbessert und erfolgreich abgeschlossen werden kann, eine zeitnahe Datenübertragung ermöglicht wird und die Kontinuität der Dienste gewährleistet bleibt. Insbesondere wird der Anbieter auf Wunsch des Kunden diesen dabei unterstützen, die Gründe für den erfolglosen Wechsel zu identifizieren, und ihn beraten, wie die identifizierten Hindernisse beseitigt oder umgangen werden können.
7.4. Nach eigenem Ermessen wird der Kunde auch den Zielanbieter einbeziehen, um den Wechselvorgang erfolgreich abzuschließen.
7.5. Wenn der Kunde nicht wechseln, sondern seine exportierbaren Daten und digitalen Vermögenswerte löschen möchte, verpflichtet sich der Anbieter, die Daten zu löschen, dies dem Kunden zu bestätigen und den Kunden nach Ablauf von 2 Monaten nach dem Löschungsverlangen über die Beendigung des Vertrags zu informieren.
7.6. Die Vereinbarung sowie die vereinbarten Dienstleistungen und Funktionen enden nicht, bevor eine der in den Ziffern 7.1.1. oder 7.1.2. beschriebenen Situationen (Ereignis A oder B) eindeutig eingetreten ist. Im Übrigen gilt die nachfolgende Ziffer 7.7.
7.7. Der Vertrag endet nicht vor dem erfolgreichen Abschluss des Wechselprozesses oder vor einer entsprechenden Entscheidung eines zuständigen Gerichts oder einer Parteivereinbarung.
7.8. Änderungen oder Ergänzungen dieser Anlage 2 bedürfen der Schriftform und beidseitiger Zustimmung.

**Anhang 1 zu Anlage 2**

**1.1. Standard-Servicegebühren:**

(Anmerkung intern: Geben Sie hier bitte Ihre Servicegebühren an)

**1.2. Die Strafen für vorzeitige Beendigung des Vertrages:** Die Höhe der Strafen für eine vorzeitige Beendigung des Vertrages entspricht den Standard-Servicegebühren, die angefallen wären, wenn der Vertrag bis zum Ende der vereinbarten Laufzeit fortgesetzt worden wäre.

(Anmerkung intern: Nach dem Data Act können die Kunden auch vor der vereinbarten Laufzeit aus dem Vertrag ausscheiden. Dann wird aber eine Vertragsstrafe fällig).

**1.3. Wechselentgelte:** Bis zum 12. Januar 2027 sind die Kosten vom Kunden zu erstatten, die dem Anbieter in unmittelbaren Zusammenhang mit dem betreffenden Wechsel entstehen. Ab dem 12. Januar 2027 werden keine Wechselentgelte mehr erhoben.

(Anmerkung intern: Nach dem Data Act entfallen die Wechselentgelte ab dem 12. Januar 2027. Vor dem 12. Januar 2027 sind die Kosten zu erstatten, die unmittelbar im Zusammenhang mit dem betreffenden Wechsel entstehen (auch z. B. Personal- oder Lizenzkosten), nicht aber die Kosten, die unabhängig von jedem Wechselvorfall anfallen (sog. Gemeinkosten).)

**1.4. Verfahren für den Wechsel:**

(Anmerkung intern: Beschreiben Sie bitte hier, wie die Kunden verfahren sollen, wenn sie den Dienst wechseln möchten. Insbesondere an wen schreiben die Kunden die Mitteilung, auch möglich per E-Mail, dass sie wechseln wollen? Welche Schritte sind erforderlich, um den Wechsel zu vollziehen?)

**1.5. Maschinenlesbare Datenformate, in denen die Nutzerdaten exportiert werden können:**

(Anmerkung intern: Geben Sie hier bitte an, in welchen Datenformaten die Nutzerdaten exportiert werden können, z. B. PDF- oder Word-Datei.)

**1.6. Instrumente für den Datenexport, einschließlich offener Schnittstellen:**

(Anmerkung intern: Geben Sie hier bitte an, über welche offene Schnittstellen der Datenexport geschieht. Sie sind nach dem Data Act verpflichtet, unentgeltlich offene Schnittstellen für die Kunden und ggf. für die neuen Anbieter der Kunden für den Datenexport bereit zu stellen. Natürlich können die Daten über die offenen Schnittstellen nur nach Authentifizierung und Autorisierung des Kunden verfügbar sein.)

**1.7. Relevante Standards auf der Grundlage offener Interoperabilitätsspezifikationen:**

(Anmerkung intern: Die Anbieter bzw. ihre Dienste müssen mit technischen Standards konform sein, die von der EU veröffentlicht werden. Die Umsetzungsfrist für Anbieter ab Veröffentlichung beträgt 12 Monate.

Auch müssen die Anbieter ihre Kunden über diese Standards informieren. Noch wurden die Standards nicht veröffentlicht, sodass Anbieter auch nicht konform oder informieren müssen. Solange keine Standards veröffentlich sind, sind die Daten in einem strukturierten, gängigen und maschinenlesbaren Format bei einem Wechselverlangen des Kunden zu exportieren, z. B. Word oder PDF-Datei (siehe 1.5.).)

**1.8. Informationen über technische Beschränkungen und Einschränkungen, die sich auf den Vollzug des Wechsels auswirken:**

(Anmerkung intern: Hier geben Sie bitte Informationen (sofern vorhanden) über technische Beschränkungen und Einschränkungen, die sich auf den Vollzug des Wechsels auswirken können.)

**1.9. Geschätzte Zeit, die erforderlich ist, um den Wechsel zu vollziehen:**

(Anmerkung intern: Hier geben Sie bitte Informationen zu der geschätzten Zeit, um den Wechsel zu vollziehen.)

**1.10. Webseite mit Online-Register, das die Datenstrukturen und -formate, relevanten Standards und offenen Interoperabilitätsspezifikationen sowie die exportierbaren Datenkategorien und digitalen Vermögenswerte enthält:**

(Anmerkung intern: Geben Sie hier bitte die Internetadresse Ihrer Webseite an (Link). Die Webseite muss Informationen zu den Datenstrukturen (wie sind die exportierbaren Daten strukturiert?), zu den Datenformaten (In welchem Format können Sie exportiert werden, z. B. Word- oder PDF-Datei?) und dazu enthalten, welche Kategorien von exportierbaren Daten und digitalen Vermögenswerten es gibt (z.B. Kundendaten). Die Webseite ist stets aktuell zu halten.)

**1.11. Webseite des Anbieters in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld:**

(Anmerkung intern: Die Vorschrift soll Transparenz darüber schaffen, aus welcher Jurisdiktion ein Zugriff auf die in Ihren Diensten gespeicherten Daten erfolgen kann und welche Schutzvorkehrungen ggf. dagegen getroffen wurden. Beispielsweise, wenn die Daten in den USA gespeichert sind und staatliche Stellen hierauf möglicherweise Zugriff haben. Geben Sie deshalb hier bitte Ihre Webseite an, die zum einen Informationen dazu enthält, welcher Gerichtsbarkeit die IKT-Infrastruktur unterliegt, die für die Datenverarbeitung Ihrer Dienste errichtet wurde (z. B. Deutschland oder die USA).

Zum anderen muss die Webseite eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen enthalten, die Sie getroffen haben, um einen internationalen staatlichen Zugang oder eine internationale staatliche Übermittlung zu verhindern, wenn ein entsprechender Zugang oder eine entsprechende Übermittlung im Widerspruch zum Unionsrecht oder zum nationalen Recht stünde. (Technische Maßnahmen sind beispielsweise Verschlüsselung der Daten und Firewalls; Organisatorische Maßnahmen sind beispielsweise Leitlinien und Mitarbeiterschulungen).)

**1.12. [Gegebenenfalls] Informationen über Datenverarbeitungsdienste**, durch die der Wechsel sehr kompliziert oder kostspielig wird oder ohne nennenswerte Eingriffe in die Daten, digitalen Vermögenswerte oder die Dienstarchitektur unmöglich ist.

(Anmerkung intern: Soweit Ihnen hierzu Informationen vorliegen, sind Ihre Kunden auch darüber zu informieren)