

Auftragsverarbeitungsvertrag

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

dotega GmbH
Freiligrathstraße 8
70372 Stuttgart

- Auftragnehmer -

und

dem jeweiligen Kunden der dotega-Dienste

- Auftraggeber –

1. Allgemeines

(1) Dieser Auftragsverarbeitungsvertrag ergänzt den zwischen dem Kunden (Auftraggeber) und der dotega GmbH (Auftragnehmer) geschlossenen SaaS-Vertrag und findet Anwendung, soweit im Rahmen der Nutzung des Dienstes personenbezogene Daten verarbeitet werden, die dem Anwendungsbereich der Verordnung (EU) 2016/679 - Datenschutz-Grundverordnung (DSGVO) unterliegen, und die dotega GmbH diese Daten als Auftragsverarbeiter im Auftrag des Kunden verarbeitet.

(2) Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

(1) Die dotega GmbH stellt dem Kunden eine Software as a Service zur Immobilien- und WEG bzw. Eigentümergemeinschaft-Verwaltung zur Verfügung und verarbeitet hierbei personenbezogene Daten im Auftrag des Kunden.

(2) Die Verarbeitung dient insbesondere der Verwaltung von Immobilien, Miet- und Eigentumsverhältnissen sowie der damit verbundenen Kommunikation, Dokumentenverwaltung und Organisation von Verwaltungsprozessen.

(3) Von der Verarbeitung können insbesondere folgende Kategorien betroffener Personen umfasst sein:

- Eigentümer

- Mieter und Bewohner
- Interessenten
- Dienstleister und Handwerker
- sonstige vom Kunden verwaltete Kontaktpersonen

(4) Von der Verarbeitung können insbesondere folgende Kategorien personenbezogener Daten umfasst sein:

- Stammdaten
- Kontaktdaten
- Vertragsdaten
- Kommunikationsdaten
- Zahlungs- und Abrechnungsdaten
- Dokumente und sonstige vom Kunden gespeicherte Inhalte

(5) Der konkrete Umfang der Verarbeitung, die eingesetzten Funktionen sowie die damit verbundenen Verarbeitungsvorgänge ergeben sich ergänzend aus den jeweils vom Kunden genutzten Leistungen und deren Beschreibung in den Nutzungsbedingungen.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Sollten die ergänzenden Weisungen des Auftraggebers beim Auftragnehmer zu erheblichen Mehraufwänden führen, darf der Auftragnehmer diese Mehraufwände dem Auftraggeber in angemessenem Rahmen in Rechnung stellen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten grundsätzlich innerhalb der Mitgliedstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR). Soweit eine Verarbeitung personenbezogener Daten in einem Drittland erforderlich wird, informiert der Auftragnehmer den Auftraggeber hierüber in Textform (z. B. per E-Mail) vor Aufnahme der Verarbeitung. Der Auftragnehmer stellt sicher, dass die Anforderungen der Art. 44 bis 49 DSGVO eingehalten werden und ein angemessenes Schutzniveau für die betroffenen personenbezogenen Daten gewährleistet ist. Der Auftraggeber ist berechtigt, der beabsichtigten Drittlandsverarbeitung innerhalb von 30 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund zu widersprechen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisaufnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die die Sicherheit der Datenverarbeitung negativ beeinflussen könnten, vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Personenbezogene Daten des Auftraggebers werden durch ein mandantenfähiges Berechtigungskonzept logisch von den Daten anderer Kunden getrennt. Nutzer können ausschließlich auf die Daten des ihnen zugeordneten Mandanten zugreifen. Eine physische Trennung der Datenbestände erfolgt nicht.

5. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

7. Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer trägt Sorge dafür, dass Beschäftigte personenbezogene Daten des Auftraggebers an mobilen Arbeitsplätzen ausschließlich auf vom Auftragnehmer bereitgestellten und verwalteten IT-Systemen (insbesondere Firmenlaptops) verarbeiten. Die Nutzung privater Endgeräte für die Verarbeitung personenbezogener Daten des Auftraggebers ist unzulässig.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer unter Wahrung der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist. Die Auskunftserteilung kann insbesondere durch die Vorlage von Unterlagen wie zum Beispiel von Prüfberichten oder Testaten erfolgen.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist (mindestens 10 Werktage) die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Etwaige Aufwendungen des Auftragnehmers für Vor-Ort-Prüfungen trägt der Auftraggeber.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(5) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist grundsätzlich zulässig.

(2) Der Auftraggeber stimmt dem Einsatz der in der folgenden Tabelle aufgeführten Unterauftragnehmer zu:

Unterauftragnehmer	Leistung	Serverstandort
Microsoft Ireland Operations Ltd	Microsoft 365, Microsoft Teams und Azure Dienste für E-Mail Kommunikation, Telefonie, Identitätsverwaltung, Zusammenarbeit und automatisierte Dokumentenanalyse	EU (Niederlande / Irland)
Amazon Web Services EMEA SARL	Ergänzende Cloud Infrastruktur, Hosting, Datensicherung und KI gestützte Datenauswertung	EU (Deutschland)
Stripe Payments Europe Ltd	Registrierung, Nutzerverwaltung, Rechnungsstellung, Zahlungseinzahlung und Zahlungsabwicklung	EU (Niederlande / Irland)
finAPI GmbH	Open Banking Schnittstelle zur Abfrage von Kontoinformationen, Zahlungsauslösung, Bankdatenverifizierung und Finanzdatenanalyse	EU (Deutschland)
Pipedrive OÜ	Vertriebs CRM, Lead und Kundenkontaktverwaltung sowie Vertriebs und Kommunikationsprozesse	EU (Deutschland, Irland, Schweden)
Zendesk Inc.	Helpdesk, Ticketverwaltung und Kundenservice Kommunikation einschließlich Chat, Wissensdatenbank und Auswertungen	EU (Irland)
Aircall SAS	Cloud Telefonie, Anrufsteuerung, Gesprächsaufzeichnungen, Voicemail und Anrufanalysen	EU (Deutschland / Irland)
Google Cloud EMEA Ltd.	Google Workspace für E-Mail, Kalender, Dateispeicherung, Dokumente, Videokonferenzen und Zusammenarbeit	EU (Deutschland)

(3) Der Auftragnehmer informiert den Auftraggeber in Textform über geplante Änderungen, insbesondere die Hinzuziehung oder den Austausch von Unterauftragnehmern. Der Auftraggeber kann einer Änderung **innerhalb von 14 Tagen nach Zugang der Mitteilung widersprechen**. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Zustimmung als erteilt. Die Parteien stimmen überein, dass diese sogenannte „Widerspruchslösung“ im Sinne von Art. 28 Abs. 2 S. 2 DSGVO zulässig ist und den operativen Erfordernissen der dotega GmbH entspricht.

(2) Der Auftragnehmer stellt vor der Beauftragung von Unterauftragnehmern durch eine risikobasierte Prüfung der verfügbaren Informationen und Nachweise sicher, dass diese ein angemessenes Datenschutzniveau gewährleisten können. Zur laufenden Überprüfung kann sich der Auftragnehmer insbesondere auf Zertifizierungen, Prüfberichte, Datenschutznachweise, Sicherheitsdokumentationen oder vergleichbare Unterlagen der Unterauftragnehmer stützen. Der Auftragnehmer dokumentiert die Durchführung dieser Prüfungen in angemessenem Umfang.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(4) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden.

(6) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den

Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

12. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 1** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

13. Dauer des Auftrags

(1) Dieser Auftragsverarbeitungsvertrag tritt mit Abschluss des SaaS-Vertrags zwischen dem Kunden und der Dotega GmbH in Kraft.

(2) Er gilt für die Dauer der Verarbeitung personenbezogener Daten im Rahmen des SaaS-Vertrags und endet automatisch mit dessen Beendigung, sofern nicht gesetzliche Aufbewahrungs- oder Nachweispflichten eine weitere Verarbeitung erfordern.

(3) Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn eine Partei

schwerwiegend oder wiederholt gegen datenschutzrechtliche Pflichten oder wesentliche Bestimmungen dieses Auftragsverarbeitungsvertrags verstößt.

14. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

15. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

16. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 – Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter hat folgende Maßnahmen gemäß Art. 32 DSGVO implementiert:

1. Zutrittskontrolle

- Abschließbare Büroräume
- Zugang nur für autorisierte Personen

2. Zugangskontrolle

- Authentifizierung über Azure Active Directory mit Multi-Faktor-Authentifizierung (MFA)
- Individuelle Benutzerkonten mit starken Passwortrichtlinien
- Automatische Sperrung nach fehlgeschlagenen Anmeldeversuchen
- Verschlüsselte Kommunikation (TLS/HTTPS)

3. Zugriffskontrolle

- Rollenbasiertes Berechtigungssystem (RBAC)
- Mandantentrennung auf Datenbankebene (Row-Level-Security)
- Minimalprinzip bei der Rechtevergabe (Least Privilege)
- Regelmäßige Überprüfung der Zugriffsberechtigungen

4. Weitergabe- und Verschlüsselungskontrolle

- Verschlüsselte Datenübertragung (TLS 1.2+)
- Verschlüsselte Datenbanken (Encryption at Rest)
- Sichere API-Kommunikation mit Authentifizierung

5. Auftragskontrolle und Zugriffshandhabung

- Schriftliche Weisungen des Verantwortlichen
- Verpflichtung der Mitarbeiter auf Vertraulichkeit
- Regelmäßige Datenschutzschulungen
- Support-Zugriffe auf Kundendaten erfolgen nur bei Bedarf und unterliegen dem Minimalprinzip

6. Verfügbarkeitskontrolle

- Regelmäßige automatisierte Backups
- Health-Check-Monitoring aller Produkktivsysteme (automatisiert, zentrale Übersicht)
- Redundante Serverinfrastruktur bei AWS
- Dokumentierte Notfall- und Wiederherstellungsverfahren

7. Patch- und Schwachstellenmanagement

- Regelmäßige Aktualisierung von Betriebssystem, Laufzeitumgebung und Abhängigkeiten
- Automatisierte Prüfung auf bekannte Schwachstellen (Dependency Scanning)
- Zeitnahe Einspielung sicherheitsrelevanter Updates

8. Trennungskontrolle

- Logische Mandantentrennung auf Datenbankebene
- Separate Datenbankinstanzen je Produkt wo erforderlich
- Getrennte Entwicklungs-, Test- und Produktivumgebungen