

Auftragsverarbeitungsvertrag

Allgemeines

Der Auftragnehmer (Robin Data GmbH, Fritz-Haber-Str. 9, 06217 Merseburg, vertreten durch den Geschäftsführer Prof. Dr. Andre Döring) verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ in Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 1. Gegenstand der Vereinbarung

1. Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:
 - Bereitstellung einer SaaS-Lösung zur Umsetzung von Compliance-Management-Systemen (ComplianceOS und dessen Module)
 - Fernwartung bei lokal installierten Komponenten oder aus Supportzwecken beim Auftraggeber
 - Verarbeitung von Kunden- und Rechnungsdaten im Auftrag.
2. Der Gegenstand des Auftrages ist darüber hinaus in den Leistungsvereinbarungen und im Hauptvertrag bzw. im Angebot benannt, welches dem Auftraggeber vorliegt.
3. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
 - Vorname, Name, E-Mail-Adresse der Nutzer der Robin Data Software (Pflichtfelder)
 - Bei System-Nutzer zusätzlich das Passwort
 - Geschlechtspronomen, Adress- und Kontaktdaten, Standortzugehörigkeit, Funktion und Rollen in der Organisation
 - Fachkundeeinformationen (DSB)
 - Personenbezogene Daten in Dokumenten-Anlagen (z. B. PDF oder Word) die der Auftraggeber in die Software hochlädt
4. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
 - Mitarbeiter des Auftraggebers
 - Kunden des Auftraggebers
 - Mitarbeiter externer Kontakte

§ 2. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Der Auftraggeber ist der Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Für die sich aus Art. 13 DSGVO ergebende Informationspflicht ist allein der Auftraggeber verantwortlich. Dem Auftragnehmer steht nach Ziff. IV Abs. 6 das Recht zu, den Auftraggeber auf eine seiner Meinung nach rechtlich unzulässigen Datenverarbeitungen hinzuweisen.

2. Der Auftraggeber kann sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeiteten Daten ein angemessenes Schutzniveau bieten.
3. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Alle Weisungen sind zu dokumentieren. Mündliche Weisungen sind unverzüglich schriftlich oder in elektronischer Form zu bestätigen.
4. Der Auftraggeber benennt dem Auftragnehmer weisungsberechtigte Personen nach Vertragsabschluss per E-Mail-Nachricht an datenschutz@robin-data.io. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in elektronischer Form mitteilen.
5. Regelungen im Hauptvertrag bzw. im Angebot über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 22 TDDDG, § 169 TKG oder Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.
8. Der Auftragnehmer stellt technische Möglichkeiten zur Verfügung, um in ComplianceOS verarbeitete personenbezogene Daten auszudrucken. Der Auftraggeber ist dafür zuständig, organisatorische Maßnahmen zur Erstellung und Nutzung von Ausdrucken personenbezogener Daten festzulegen.

§ 3. 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 dokumentierten Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den dokumentierten Weisungen des Auftraggebers. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, es liegt es ein Fall des Art. 28 Abs. 3 Buchst. a) DSGVO vor. In diesem Fall hat der Auftragnehmer den Auftraggeber vorab über diese Verpflichtung zu informieren, es sei denn, ein wichtiges öffentliches Interesse verbietet ihm dies. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen hiervon sind Sicherungskopien.
2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber unter Angabe von Namen, Organisationseinheit, Funktion und Telefonnummer die Personen schriftlich oder elektronisch mitzuteilen, die zur Entgegennahme von Weisungen des Auftraggebers befugt sind oder als Ansprechpartner fungieren. Änderungen sind dem Auftraggeber unverzüglich schriftlich mitzuteilen.

Zur Entgegennahme von Weisungen ist berechtigt:

- Prof. Dr. Andre Döring (datenschutz@robin-data.io, 03461 – 479236-0)
 - Nadine Porrmann (datenschutz@robin-data.io, 03461 – 479236-0)
3. Soweit Datenträger vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, sind sie besonders zu kennzeichnen. Eingang und Ausgang derer werden in geeigneter Weise dokumentiert.

4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
5. Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen von Art. 32 DSGVO genügen. Diesbezüglich wird auf § 10, Technische und Organisatorischen Maßnahmen zur Datensicherheit, verwiesen.
6. Der Auftragnehmer überprüft regelmäßig die auftrags- und datenschutzgerechte Durchführung dieses Vertrages, mindestens jedoch einmal jährlich. Die Prüfergebnisse sind zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen.
7. 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. 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.

Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben enthalten.

Der Auftragnehmer verpflichtet sich, sämtliche Offenlegungen personenbezogener Daten gegenüber Dritten zu dokumentieren – unabhängig davon, ob diese im Rahmen des regulären Systembetriebs oder aufgrund besonderer Umstände erfolgen. Zu den aufzuzeichnenden Informationen zählen mindestens die Art der offengelegten personenbezogenen Daten, die Identität der empfangenden natürlichen oder juristischen Person, das Datum und die Uhrzeit der Offenlegung, die Rechtsgrundlage oder der berechtigte Zweck der Offenlegung, die Quelle der Entscheidung zur Offenlegung (z. B. auf Weisung des Verantwortlichen oder aufgrund gesetzlicher Verpflichtung). Auch Offenlegungen, die im Zuge rechtlicher Untersuchungen, behördlicher Auskunftersuchen oder externer Audits erforderlich werden sind ebenfalls vollständig und nachvollziehbar zu dokumentieren. Der Auftraggeber hat jederzeit das Recht, Einsicht in diese Aufzeichnungen zu nehmen oder eine Kopie anzufordern.

8. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform (Fax/E-Mail) zulässig. Davon ausgenommen ist eine Verarbeitung von Daten für den Auftraggeber außerhalb von Betriebsstätten des Auftragnehmers von dafür vom Auftragnehmer eingesetzten Mitarbeitern, soweit mit dieser häuslichen Telearbeit oder mobiles Arbeiten vereinbart wurde. Der Auftragnehmer hat jedoch in jedem Fall die Einhaltung der organisatorisch-technischen Maßnahmen sicherzustellen.
9. Der Auftragnehmer ist verpflichtet, Beschwerden und Eingaben, die er im Zusammenhang mit diesem Vertrag erhält, unverzüglich an den Auftraggeber weiterzuleiten.
10. An der Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
11. Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. § 38 BDSG (neu) bestellt bzw. nach Art. 37 DSGVO benannt hat. Die Pflicht zur Bestätigung kann im

Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

12. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.
13. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.
14. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung so weit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
15. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag bereits vereinbart.

§ 4. Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer ist als Beauftragter für den Datenschutz

- Rechtsanwalt Richard Bode, Dresden, datenschutz@robin-data.io

bestellt. Ein Wechsel des Beauftragten für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

§ 5. 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 jederzeit 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.
3. Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.
4. Der Auftraggeber kann grundsätzlich nach vorheriger Anmeldung mit angemessener Frist 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.

5. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber Art. 58 DSGVO, insbesondere im Hinblick auf Auskunftspflichten 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.

§ 6. Unterauftragsverhältnisse

1. Der Auftraggeber erteilt dem Auftragnehmer hiermit eine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO, Unterauftragsverarbeiter im Rahmen der Erbringung der vertraglich vereinbarten Leistungen einzusetzen. Die zum Zeitpunkt der Unterzeichnung dieses Vertrages beauftragten Unterauftragsverarbeiter ergeben sich aus Anlage 2.
2. Der Auftragnehmer informiert den Auftraggeber vorab in Textform über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Die Information hat so rechtzeitig zu erfolgen, dass dem Auftraggeber eine angemessene Frist zur Prüfung und zur Erhebung eines Einspruchs verbleibt.
3. Der Auftraggeber ist berechtigt, binnen 14 Tagen ab Zugang der Information aus wichtigem datenschutzrechtlichem Grund gegen die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters Einspruch zu erheben. Legt der Auftraggeber Einspruch ein, werden die Parteien sich in diesem Fall unverzüglich und nach Treu und Glauben darum bemühen, eine einvernehmliche Lösung zu finden. Eine solche Lösung kann insbesondere darin bestehen, dass der Auftragnehmer auf den Einsatz des betreffenden weiteren Auftragsverarbeiters verzichtet, einen alternativen weiteren Auftragsverarbeiter einsetzt oder durch geeignete zusätzliche technische und organisatorische Maßnahmen die vom Auftraggeber geltend gemachten datenschutzrechtlichen Bedenken ausräumt. Kann eine einvernehmliche Lösung nicht erzielt werden, ist jede Partei berechtigt, den Vertrag oder, soweit abgrenzbar, den hiervon betroffenen Leistungsteil zum geplanten Zeitpunkt der Übergabe der im Auftrag für den Auftraggeber verarbeiteten zu kündigen. Der Auftragnehmer hat den Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Unterauftragsverarbeiter gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
4. Der Auftragnehmer hat mit dem Unterauftragsverarbeiter einen Auftragsverarbeitungsvertrag zu schließen, durch den dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt werden, die in diesem Vertrag zwischen Auftraggeber und Auftragnehmer festgelegt werden. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
5. Nicht als Unterauftragsverhältnisse 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. Wartungs- und Prüfungsleistungen stellen keine zustimmungspflichtigen Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung der IT-Systeme nicht schwerpunktmäßig die Verarbeitung personenbezogener Daten zum Inhalt hat.

§ 7. Datengeheimnis / Vertraulichkeitsverpflichtung

1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 53 BDSG (neu) bzw. nach Art. 28 Abs. 3 Buchst. b) DSGVO zu Wahrung der Vertraulichkeit verpflichtet. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.
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 die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 53 BDSG (neu) bzw. nach Art. 28 Abs. 3 Buchst. b) DSGVO verpflichtet werden. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 3 TDDDG zu verpflichten.
3. Diese Verpflichtung der beschäftigten Mitarbeiter ist auf Anfrage dem Auftraggeber nachzuweisen.

§ 8. Geheimhaltungspflichten

1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 9. Vergütung

1. Für anlassbezogene Kontrollen, Prüfungen, Abforderung von Dokumentationen oder Unterstützungsleistungen, insbesondere Mitwirkungspflichten des Auftragnehmers an bzw. für den Auftraggeber fällt keine zusätzliche Vergütung an.
2. Für anlasslose Kontrollen, Prüfungen, Vorlage von Dokumentationen oder abgeforderten Unterstützungsleistungen sowie Mitwirkungspflichten des Auftragnehmers an bzw. für den Auftraggeber zahlt der Auftraggeber dem Auftragnehmer als Aufwandsentschädigung je Vorgang und Zeitdauer der dadurch bedingten Inanspruchnahme einen Stundensatz in Höhe von 150 € netto zzgl. der gesetzlichen Mehrwertsteuer.

§ 10. Technische und organisatorische Maßnahmen zur Datensicherheit

1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber nach den Art. 28 Abs. 3 Buchst. c) und Art. 32 DSGVO technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.
2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 1 zu diesem Vertrag beigelegt. 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 Vorweg mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nie unterschritten werden. Alle wesentlichen Änderungen sind zu dokumentieren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
3. Der Auftragnehmer implementiert Verfahren zur sicheren Registrierung, Verwaltung und Deregistrierung von Benutzerkonten. Diese Verfahren beinhalten insbesondere Vorkehrungen zur Reaktion auf Sicherheitsvorfälle im Zusammenhang mit der Kompromittierung von Benutzerzugängen. Im Einzelnen gelten folgende Maßnahmen:
 - **Registrierung und Deregistrierung**

Benutzerkonten werden ausschließlich auf dokumentierte Anforderung des Verantwortlichen eingerichtet. Die Deregistrierung erfolgt unverzüglich nach Entzug der Berechtigung oder bei Vertragsbeendigung.
 - **Zugangsschutz und Authentifizierung**

Zugänge zur SaaS-Anwendung sind durch starke Authentifizierungsmechanismen geschützt (z.B. starke Passwortrichtlinien, optional Zwei-Faktor-Authentifizierung).
 - **Kompromittierungsmanagement**

Für den Fall der Verfälschung oder Kompromittierung von Zugangsdaten (z.B. infolge unbeabsichtigter Offenlegung, Phishing oder anderer Angriffe) bestehen dokumentierte Prozesse zur:

 - unverzüglichen Sperrung des betreffenden Kontos,
 - Benachrichtigung des Verantwortlichen,
 - forcierten Rücksetzung aller betroffenen Authentifizierungsdaten,
 - Analyse und Protokollierung des Vorfalls im Sicherheitsmanagementsystem.
 - **Benutzerbenachrichtigung und Eskalation**

Der betroffene Benutzer sowie der Verantwortliche werden im Falle einer bestätigten oder vermuteten Kompromittierung unverzüglich informiert. Die weitere Kommunikation erfolgt gemäß den internen Sicherheitsrichtlinien und vertraglichen Meldefristen.

- **Protokollierung**

Alle sicherheitsrelevanten Änderungen an Benutzerkonten, insbesondere Registrierung, Passwortänderungen, Sperrungen und Deregistrierungen, werden nachvollziehbar protokolliert und regelmäßig überprüft.

4. 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.
5. Werden durch den Auftraggeber personenbezogene Daten über die API-Schnittstelle abgerufen, ist der Auftraggeber selbst für die Verarbeitung verantwortlich. Der Auftragnehmer stellt sicher, dass der Auftraggeber über die API ausschließlich die über den API-Key berechtigten Daten des zugehörigen Mandanten abrufen kann.

§ 11. Dauer des Auftrags

1. Der Vertrag beginnt mit der vereinbarten Laufzeit aus dem Hauptvertrag bzw. dem Angebot und wird auf unbestimmte Zeit geschlossen. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages bzw. des Angebotes, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.
2. Die ordentliche Kündigung dieses Vertrages ist für die Dauer des Hauptvertrages ausgeschlossen.
3. Das Recht zum Ausspruch einer außerordentlichen Kündigung durch die Parteien wird durch vorstehende Bestimmungen nicht eingeschränkt. Der Auftraggeber kann den Vertrag insbesondere jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert. Der Auftragnehmer kann den Vertrag insbesondere jederzeit kündigen, wenn ein schwerwiegender Verstoß des Auftraggebers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftraggeber die vertraglich vereinbarte Vergütung trotz erfolgloser Nachfristsetzung nicht zahlt oder an offensichtlich rechtswidrigen Weisungen zur Datenverarbeitung trotz entsprechendem Hinweis des Auftragnehmers festhält.

§ 12. Haftung

1. Für Schadenersatzansprüche, die Betroffene gegenüber dem Auftragnehmer wegen eines Verstoßes aus diesem Vertrag geltend machen, gilt die gesetzliche Regelung. Gegenüber betroffenen Personen haften Auftraggeber und Auftragnehmer gemäß der in Art. 82 DSGVO getroffenen Bestimmung.
2. Der Auftraggeber stellt den Auftragnehmer im Innenverhältnis von sämtlichen Ansprüchen Dritter (z.B. von Betroffenen, Aufsichtsbehörden etc.) frei, die daraus resultieren, dass eine Verletzung dieses Vertrages und/oder gesetzlicher datenschutzrechtlicher Bestimmungen allein oder überwiegend auf ein Verhalten des Auftraggebers zurückzuführen ist.
3. Schadenersatzansprüche des Auftraggebers gegen den Auftragnehmer im Innenverhältnis wegen einer Pflichtverletzung aus diesem Vertrag sind unabhängig vom Rechtsgrund ausgeschlossen, es sei denn, der Auftragnehmer, seine gesetzlichen Vertreter oder Erfüllungsgehilfen haben vorsätzlich oder grob fahrlässig gehandelt.

Für leichte Fahrlässigkeit haftet der Auftragnehmer nur, wenn eine für die Erreichung des Vertragszwecks wesentliche Vertragspflicht durch den Auftragnehmer, seine gesetzlichen Vertreter

oder leitenden Angestellten oder Erfüllungsgehilfen verletzt wurde, sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit. Der Auftragnehmer haftet dabei nur für vorhersehbare Schäden, mit deren Entstehung typischerweise gerechnet werden muss. Dafür ist seine Haftung auf einen Maximalbetrag in Höhe von € 100.000 beschränkt.

Als Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag stehenden Streitigkeiten wird Merseburg vereinbart.

§ 14. Beendigung

1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse außerhalb der ComplianceOS, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen bzw. datenschutzkonform zu löschen, sofern keine gesetzlichen Regelungen dem widersprechen oder eine andere Regelung getroffen wird.

Die gespeicherten Daten im ComplianceOS zu diesem Auftragsverhältnis werden nach Beendigung des Vertragsverhältnisses auf Antrag des Auftraggebers, sofern technisch möglich, datenschutzkonform gelöscht oder gesperrt.

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage geeignete Informationen zur Verfügung, die es diesem ermöglichen, die vollständige und nachweisbare Löschung aus allen relevanten Speicherorten – auch bei Unterauftragnehmern – zu überprüfen und zu dokumentieren.

2. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

§ 15. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB 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 zu diesem Vertrag ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

§ 17. Zugang der Aufnahmeerklärung

Der Auftragnehmer verzichtet auf den Zugang der Annahmeerklärung für die Vertragswirksamkeit.

Merseburg, den 15.07.2026 | 13:45:50 MESZ

Signiert von:



Geschäftsführung

DocuSigned by:

ADöring
C65176A51E804E4...

Prof. Dr. Andre Döring

Anlagen

- Anlage 1: TOM-Liste
- Anlage 2: Liste der Subunternehmer

Technische und organisatorische Maßnahmen (TOMs)

i. S. d. Art. 32 DSGVO

Robin Data folgende technisch-organisatorische Maßnahmen zum Datenschutz um:

- Robin Data ist nach ISO / IEC 27001:2022, ergänzt mit ISO / IEC 27017 und ISO / IEC 27018 sowie der ISO 9001:2015 zertifiziert. Das Statement of Applicability der ISO / IEC 27001-Zertifizierung kann auf Anfrage ausgehändigt werden. Regelungen, die hier erfasst sind werden im folgende nicht weiter ausgeführt.
- Verzeichnis der Verarbeitungstätigen nach Art. 30 DSGVO und Umsetzung etwaiger Anforderungen nach Art. 35 DSGVO
- Benennung eines Datenschutzbeauftragten.
- Löschkonzept zur Umsetzung von Art. 17 DSGVO mit manuellen und automatischen Löschroutinen
- Verpflichtungen der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Mitarbeiterschulungen zum Datenschutz und zu Informationssicherheit
- Entgegennehmen ausschließlich schriftlicher Weisungen des Auftraggebers
- Privacy-by-Design und Security-by-Design bei der Softwareentwicklung
- Verbindliche Regelungen zum mobilen Arbeiten sind erlassen und Verschlüsselung mobiler Geräte und MDM sowie Endpoint-Protection.
- Einsatz eines Secure-Mail-Gateways zur sicheren E-Mail-Kommunikation.
- Ausschließliches Hosting und Betrieb des SaaS-Lösung in deutschen ISO / IEC 27001 zertifizierten Rechenzentren, durch eigenes Personal in einer durch Robin Data kontrollierten Serverumgebung.
- Minimierung von Administratorzugängen
- Anonymisierte Auswertung von Nutzerstatistiken des ComplianceOS
- Perimeterschutz durch Transponderregelungen und Secure-Cage zur Sicherung sensibler Daten und Technik im Büro
- Umsetzung von Rollen- und Rechtemanagement in allen Anwendungen die personenbezogenen Daten verarbeiten
- Clean-Desktop-Philosophie und Reinigungspersonal während der Bürozeiten unter Aufsicht.
- Sichere Anmeldeverfahren (FIDO-Authentifizierung)
- UFA bzw. 2FA in allen Anwendungen, wenn möglich.
- Automatisches Backup der IT-Systeme
- Trennung von Entwicklungs-, Test- und Betriebsumgebung
- Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
- Verschlüsselung (in transit und at rest)
- Benutzerzugangsverwaltung durch den Auftraggeber

Liste der Subunternehmer

Robin Data ComplianceOS verwendet folgende Subunternehmen:

Nr.	Unternehmen	Server-Standort	Art der Leistung
1	Amazon Webservices EMEA SARL Niederlassung Deutschland Marcel-Breuer-Str. 12 80807 München	DE	Bereitstellung der Domain „secureapp.robin-data.io“ und der benötigten Zertifikate. Wir haben einen Auftragsverarbeitungsvertrag abgeschlossen. AWS ist nach dem EU-US-Privacy-Framework zertifiziert.
2	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	DE	Betrieb der Applikations- und Datenbankumgebung von ComplianceOS. Wir haben einen Auftragsverarbeitungsvertrag abgeschlossen.

Abschlusszertifikat

Umschlag-ID: 905E456C-462C-818A-8099-711F0846606A

Status: Abgeschlossen

Betreff: Mit Docusign abschließen: AV Robin Data ComplianceOS_13.07.26.docx

Quellumschlag:

Dokumentenseiten: 12

Signaturen: 1

Umschlagersteller:

Zertifikatsseiten: 1

Initialen: 0

Andre Döring

Signatur mit Anleitung: Deaktiviert

Stempel: 1

Fritz-Haber-Str. 9

Umschlag-ID-Stempel: Deaktiviert

Merseburg, Merseburg 06217

Zeitzone: (UTC+01:00) Amsterdam, Berlin, Bern,

ado@robin-data.io

Rom, Stockholm, Wien

IP-Adresse: 2003:e6:3f23:76

Eintragsverfolgung

Status: Original

Inhaber: Andre Döring

Standort: DocuSign

15.07.2026 13:44:23

ado@robin-data.io

Unterzeichnerereignisse

Signatur

Zeitstempel

Andre Döring

DocuSigned by:

C65176A51E804E4...

Gesendet: 15.07.2026 13:44:42

ado@robin-data.io

Eingesehen: 15.07.2026 13:44:48

Geschäftsführer

Signiert: 15.07.2026 13:45:50

Robin Data GmbH



Selfservice-Signieren

Sicherheitsstufe: E-Mail, Kontoauthentifizierung
(keine)

Signaturübernahme: Auf Gerät gezeichnet

Mit IP-Adresse:

2003:e6:3f23:7600:99bc:7986:54de:a68

Vereinbarung bezüglich elektronischer Unterlagen und Signaturen:

Nicht über Docusign angeboten

Vor-Ort-Unterzeichner – Ereignisse	Signatur	Zeitstempel
Bearbeiterversandereignisse	Status	Zeitstempel
Beauftragtenzustellereignisse	Status	Zeitstempel
Vermittlerversandereignisse	Status	Zeitstempel
Zertifizierter Versand - Ereignisse	Status	Zeitstempel
Kopienereignisse	Status	Zeitstempel
Zeugen-Ereignisse	Signatur	Zeitstempel
Notarereignisse	Signatur	Zeitstempel
Umschlagereignisse – Überblick	Status	Zeitstempel
Umschlag gesendet	Hash-codiert/verschlüsselt	15.07.2026 13:44:43
Zertifiziert zugestellt	Sicherheitsprüfung ausgeführt	15.07.2026 13:44:48
Signiervorgang abgeschlossen	Sicherheitsprüfung ausgeführt	15.07.2026 13:45:50
Abgeschlossen	Sicherheitsprüfung ausgeführt	15.07.2026 13:45:50
Zahlungen	Status	Zeitstempel