Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Stand 25.11.2020, Version 1.2

1 Gegenstand und Dauer der Vereinbarung

Der Vertragspartner (im Folgenden „Kunde“ oder „Auftraggeber“) schließt zur Nutzung der Robin Data Software mit der Robin Data GmbH, Fritz-Haber-Str. 2, 06217 Merseburg, Deutschland (im Weiteren „Robin Data“ oder „Auftragnehmer“), folgenden Vertrag gemäß Art. 28 DSGVO ab.

Im Rahmen der Auftragsverarbeitung führt Robin Data folgende Dienstleistungen aus:

- Bereitstellung der Robin Data Software über einen Cloud-Dienst als Software-as-a-Service-Lösung
- Verarbeitung von Daten der Kunden im Auftrag

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Abs. 2 (Begriffsbestimmung „Verarbeitung“) und Art. 28 DSGVO (Regelungen für Auftragsverarbeiter) auf Grundlage dieses Vertrages.

1.1 Vereinbarte Dienstleistung der Auftragsverarbeitung

Die vertraglich vereinbarte Dienstleistung wird in Staaten innerhalb und außerhalb der Europäischen Union erbracht. Nähere Informationen finden sich in der Datenschutzerklärung und die Anlage 1 – Liste der Subunternehmer.

1.2 Verlagerung von Dienstleistungen in ein Drittland

Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO (Regelungen zur Übermittlung personenbezogener Daten in Drittländer oder internationale Organisationen) erfüllt sind. Dieses sind z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln oder genehmigte Verhaltensregeln.

1.3 Dauer des Auftrags

Die Dauer des Auftrags richtet sich nach dem abgeschlossenen Abonnement gemäß der AGB von Robin Data.

Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO (Regelungen für Auftragsverarbeiter) abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Jede Verarbeitung personenbezogener Daten muss nach Art. 5 Abs. 2 DSGVO auf Basis festgelegter, eindeutiger und legitimer Zwecke erfolgen.

2.1 Zweckbindung der Auftragsverarbeitung

Diese Auftragsverarbeitung basiert gemäß Artikel 5 Abs. 1 lit. b DSGVO auf dem Zwecken:

- Bereitstellung einer Datenschutz-Managementsoftware zur elektronischen Verwaltung der notwendigen Datenschutzdokumentation des Auftraggebers
- Verarbeitung der hierzu notwendigen Benutzer- und Personendaten der vom Auftraggeber in das System eingegebenen Personen
- Anonymisierte Auswertung von Nutzungsstatistiken der verarbeiteten Kundendaten durch Robin Data

2.2 Rechtsgrundlagen der Verarbeitung

Diese Auftragsverarbeitung basiert auf einer vertraglichen Grundlage (Abonnement des Kunden) gemäß Artikel 6 Abs. 1 lit. b DSGVO.

Ferner basiert die Auswertung der anonymisierten Nutzerstatistiken auf einem berechtigten Interesse gemäß Basis Artikel 6 Abs. 1 lit. f. Das berechtigte Interesse von Robin Data besteht darin, dass die Präzision der bereitgestellten Vorlagen für alle Nutzer stetig verbessert werden soll. Es werden technologisch keine konkreten Nutzerdaten verarbeitet.

2.3 Art der Verarbeitung

Entsprechend der Definition von Art. 4 Abs. 2 DSGVO (Begriffsbestimmung „Verarbeitung“) kommen folgende Verarbeitungsvorgänge in diesem Vertrag zur Anwendung:

☒	Erheben personenbezogener Daten	☒	Erfassen personenbezogener Daten
☐	Organisieren personenbezogener Daten	☒	Ordnen personenbezogener Daten
☒	Speichern personenbezogener Daten	☒	Anpassen personenbezogener Daten
☒	Auslesen personenbezogener Daten	☒	Abfragen personenbezogener Daten
☒	Verändern personenbezogener Daten	☒	Verwenden personenbezogener Daten
☐	Offenlegung personenbezogener Daten*	☐	Verbreitung personenbezogener Daten
☐	Andere Formen der Bereitstellung personenbezogener Daten	☐	Abgleich und Verknüpfung personenbezogener Daten*
☐	Einschränkung personenbezogener Daten	☒	Löschung personenbezogener Daten
☐	Vernichtung personenbezogener Daten	☐	
☐	Wobei eine Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO aufgrund folgender konkreter Verarbeitungsvorgänge durchgeführt wurde:		
Mit *-gekennzeichnete Verarbeitungsprozesse ziehen sehr wahrscheinlich eine Datenschutzfolgeabschätzung nach sich			

2.4 Datenkategorien der verarbeiteten personenbezogenen Daten

Entsprechend der Definition von Art. 4 Abs. 1, 13, 14 und 15 DSGVO (Begriffsbestimmungen „Personenbezogene Daten, genetische Daten, biometrische Daten, Gesundheitsdaten“) werden folgende Kategorien personenbezogener Daten verarbeitet:

- Vorname, Name, E-Mailadresse der Nutzer der Robin Data Software (Pflichtfelder)
- Bei Systemnutzern zusätzlich das Passwort
- Geschlecht, weitere Adress- und Kontaktdaten, Standortzugehörigkeit, Funktion und Rollen in der Organisation der Nutzer der Robin Data Software (Optionale Felder),
- Fachkunde des Datenschutzbeauftragten (Optionale Angabe)
- Analog wie oben als personenbezogene Daten für externe Kontakte der Nutzer der Robin Data Software
- Vertragsdaten von Vertragspartnern, die von den Nutzern selbst hochgeladen werden
- Ggf. Fotos und andere Dateien mit personenbezogenen Daten die von den Nutzern selbst hochgeladen werden

2.5 Kategorien der betroffenen Personen

Entsprechend der Definition von Art. 4 Abs. 1 DSGVO (Begriffsbestimmung „Personenbezogene Daten“) werden personenbezogene Daten folgender Betroffenengruppen verarbeitet:

- Mitarbeiter des Auftraggebers
- Externe Kontakte (z. B. Externer Datenschutzbeauftragter, Dienstleister- und Lieferantenmitarbeiter, Behördenmitarbeiter)

3 Rechte, Pflichten und Weisungsbefugnisse des Auftraggebers

Auf Grundlage von Art. 28 Abs. 3 lit. a (Regelungen zu „Auftragsverarbeiter“) ist ein maßgebliches Kriterium für eine Auftragsverarbeitung, dass der Auftragnehmer nur nach dokumentierter Weisung des Auftraggebers personenbezogene Daten innerhalb der EU oder in einem Drittland verarbeiten darf.

Liegt kein weisungsgebundenes Vertragsverhältnis zwischen Auftragnehmer und Auftraggeber vor, handelt es sich nicht um ein Auftragsverarbeitungsverhältnis und muss nicht über diesen Vertrag geregelt werden. Anderweitig werden die sich aus diesem Weisungsverhältnis ergebenden Rechte, Pflichten und relevanten Ansprechpartner im Folgenden festgelegt.

Verantwortlichkeit für die Zulässigkeit der Verarbeitung und die Rechte der Betroffenen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO (Regelungen zur „Rechtsmäßigkeit der Verarbeitung“) sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO (Regelungen zu den „Rechten der Betroffenen“ im Umgang mit ihren personenbezogenen Daten) ist allein der Auftraggeber verantwortlich. Der Auftragnehmer ist verpflichtet alle Anfragen die ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Meldung von Auftragsänderungen

Änderungen an der Art der Verarbeitung (z. B. Änderungen an der Art der Dienstleistung, dem Verarbeitungsgegenstand oder an Verfahrensänderungen der Zusammenarbeit) sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich (z. B. per Brief) oder in einem dokumentierten elektronischen Format (z. B. per E-Mail oder digitalem Workflow) festzulegen.

Schriftliche Erteilung von Aufträgen, Teilaufträgen und Weisungen

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Prüfung der Datensicherheit durch den Auftraggeber

Der Auftraggeber ist berechtigt, sich wie unter Abschnitt 6 festgelegt vor Beginn der Verarbeitung und so-dann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Umgang mit Fehlern und Unregelmäßigkeiten

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder der Verarbeitung personenbezogener Daten feststellt.

Geheimnisschutz auch über die Dauer des Auftrags hinaus

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

3.1 Regelung der Weisungsberechtigungen und Ansprechpartner

Es werden folgende Ansprechpartner mit Weisungsberechtigung und zum Weisungsempfang beim Auftragnehmer benannt. Diese Ansprechpartner je Partei vertreten sich in vollem Umfang gegenseitig.

1) Prof. Dr. Andre Döring, Geschäftsführer Robin Data
2) Daniel Ramsch, Kaufm. Leiter Robin Data

Robin Data ist berechtigt bei Weisungen seitens des Auftraggebers die Identität und Legitimation Anweisenden zu überprüfen.

Weisungen an Robin Data erfolgen immer formlos und in schriftlicher Form unter Angabe der Identität und Legitimation des Weisenden an folgende E-Mail-Adresse:

- datenschutz@robin-data.io

Mündliche Weisungen werden nicht akzeptiert.

4 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

Eigenmächtiges erzeugen von Duplikaten und Kopien ist nicht gestattet

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten, außer für Backups im Rahmen der IT-Sicherheit, werden ohne Wissen des Auftraggebers nicht erstellt.

Das Trennungsgebot muss beachtet werden

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt durch logische Trennung getrennt werden.

4.1 Rechte der Betroffenen im Rahmen der Auftragsverarbeitung

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 lit e und f DSGVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

4.2 Kontrollen beim Auftragnehmer durch den Auftraggeber

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 lit. h DSGVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres vereinbart, dass Kontrollen mindestens 6 Wochen vor der Durchführung in den üblichen Geschäftszeiten angemeldet werden. Der Inhalt der Kontrolle selbst muss vorher angezeigt werden. Die Kontrolle wird immer durch einen Mitarbeiter von Robin Data begleitet. Die Einsicht in Geschäftsgeheimnisse von Robin Data ist ausgeschlossen.

4.3 Heim- und Telearbeit beim Auftragnehmer

Robin Data ermöglicht seinen Mitarbeitern die Umsetzung alternierender Teleheimarbeit. Die Mitarbeiter unterliegen einer betrieblichen Vereinbarung zur Teleheimarbeit, die alle relevanten Aspekte zum Datenschutz und zur Datensicherheit regelt.

Der Zugriff auf die Daten von Robin Data oder ggf. des Auftraggebers erfolgt hierbei über einen gesicherten Dienstrechner über eine verschlüsselte Verbindung auf die Datenspeicher von Robin oder die Robin Data Software.

4.4 Regelkenntnis und besondere Geheimschutzregeln

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

4.5 Datenschutzorganisation beim Auftragnehmer

Robin Data hat einen externen betrieblichen Datenschutzbeauftragten bestellt:

R.echt Bode Rechtsanwaltskanzlei
Rechtsanwalt Richard Bode
Königsbrücker Str. 124
01099 Dresden
Fon (+49) 0351 – 41882207
Mail datenschutz@robin-data.io

Weiterhin verpflichtet sich der Auftragnehmer sofern einschlägig, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

4.6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit, sofern sie im Kontext dieses Vertrages geschehen.

Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

5 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 lit. d DSGVO)

Die Beauftragung von Subunternehmern kann durch den Auftragnehmer auf Basis eigenen Ermessen durchgeführt werden. Die Beauftragung wird dem Auftraggeber als Anlage 1 dieses Vertrags zur Kenntnis gegeben. Der Auftragnehmer wird dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Robin Data verpflichtet sich gemäß Artikel 28 Abs. 4 Subunternehmer angemessen auszuwählen und die dafür soweit es uns möglich ist auf die Einhaltung der gesetzlichen Datenschutzvorschriften hinzuwirken und die Umsetzung nach eigenem Ermessen zu kontrollieren. Aufträge mit Subunternehmern als Auftragsverarbeitern werden schriftlich gefasst.

Liste genehmigter Subunternehmer

Zurzeit sind für den Auftragnehmer folgende in Anlage 1 bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

6 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Aktuell wird die Sicherheit der Verarbeitung bei Robin Data durch technisch-organisatorische Maßnahmen umgesetzt, die in Anlage 2 dargelegt sind. Derzeit befindet sich die Umsetzung und Zertifizierung eines ISMS auf Basis ISO/IEC 27001 in der Projektierung (Zeit zur Zertifizierung ist Februar 2021).

7 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 lit. g DSGVO

Für den Umgang mit personenbezogenen Daten nach Abschluss der Auftragsverarbeitungsverhältnisses wird folgende Regelung getroffen:

- Mandanten der Robin Data Software werden 30 Tage nach Bedingung des Abonnements endgültig gelöscht

- Physische Datenträger werden durch einen professionellen Datenensorger auf Basis DIN 66399 entsorgt.

Löschungen werden gemäß DIN 66398 in im Löschkonzept dokumentiert und dem Auftraggeber gegenüber schriftlich per E-Mail bestätigt.

8 Vergütung, Haftung, Vertragsstrafen und sonstiges

Es werden folgende sonstige Regelungen für dieses Auftragsverarbeitungsverhältnis getroffen:

8.1 Vergütung

Sollte eine Vor-Ort-Kontrolle des Auftraggebers einen erheblichen im Vorfeld abzusehenden Aufwand bei Robin Data erzeugen, so ist die Arbeitsstunde eines Mitarbeiters von Robin Data zu vergüten. Hierzu wird dann ein entsprechendes Angebot erstellt.

8.2 Haftung

Es gelten die Regelungen des Art. 82 DSGVO.

8.3 Vertragsstrafen

Vertragsstrafen werden ausgeschlossen.

8.4 Sonstige Regelungen

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

9 Salvatorische Klausel

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

10 Zugang der Annahmeerklärung

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

Liste Subauftragnehmer

Anlage 1 zum Auftragsverarbeitungsvertrag der Robin Data Software. Die Liste ist gültig seit dem Datum: 04.11.2019

Nr.	Subunternehmer (Name, Anschrift)	Zweck des Auftrags	DSGVO Nachweise
1	Amazon Webservices, Frankfurt	Bereitsstellung IaaS für Robin Data App	Verarbeitung basiert auf EU Standardvertragsklauseln genehmigt durch die Artikel 29 Gruppe der EU
2	SevDesk GmbH, 77652 Offenburg	Rechnungslegung und Buchhaltung	Auftragsverarbeitungsvertrag
3	Mailgun, San Francisco (USA)	Mailing aus der Robin Data Software	Auftragsverarbeitungsvertrag (in der Umstellung auf anderen Anbieter)
4	HubSpot, 10234 Berlin	Website, CRM-System	Verarbeitung basiert auf EU Standardvertragsklauseln genehmigt durch die Artikel 29 Gruppe der EU, Auftragsverarbeitungsvertrag
5	Microsoft Inc.	Office 365	Verarbeitung basiert auf EU-Standardvertragsklauseln genehmigt durch die Artikel 29 Gruppe der EU
6	Zoom Video Communications, Inc.	Zoom Video-Konferenzen	AV abgeschlossen (Server EU)
7	Elopage GmbH	Vertrieb Online-Produkte	AV abgeschlossen
8	Usercentrics GmbH	Consent-Management	AV abgeschlossen

Dokumentation Technisch-Organisatorischer-Maßnahmen

Anlage 2 zum Auftragsverarbeitungsvertrag der Robin Data Software.

Diese Checkliste ist eine Dokumentation des Verantwortlichen im Rahmen Datenschutz-Management-Systems des Verantwortlichen.

Die Dokumentation basiert auf folgenden Anforderungen der Datenschutz-Grundverordnung (DSGVO):

- Art. 5 DSGVO -Grundsätze für die Verarbeitung personenbezogener Daten
- Art. 24 DSGVO - Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 25 DSGVO- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art 32 DSGVO – Sicherheit der Verarbeitung

Bei der Auswahl und Umsetzung der Maßnahmen kommt es im Einzelfall darauf an, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Die Aufzählung ist nicht abschließend und kann ergänzt werden. Bei Auftragsverarbeitungen, Vergabe von Unteraufträgen oder Fernwartungsaufträgen sind die Maßnahmen der Auftragsverarbeiter in einer gesonderten Anlage aufzuführen.

Folgende Abschnitte präzieren die technisch-organisatorischen Maßnahmen des Verantwortlichen zur Einhaltung der einschlägigen Vorschriften der DSGVO.

1 Transparenz

Die DSGVO verfolgt das Ziel, Betroffenen zu ermöglichen die Art und Weise der Verarbeitung ihrer personenbezogenen Daten zu verstehen und nachvollziehen zu können. Dazu gehört zum Beispiel die Möglichkeit Auskünfte darüber einzuholen, wie personenbezogene Daten durch einen verantwortlichen Verarbeiter verarbeitet und an wen diese weitergegeben werden.

Diese Transparenz im Sinne des Art. 5 Abs. 1 lit. a DSGVO ist gewährleistet, wenn die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dazu muss der Verantwortliche gemäß Art. 12 Abs. 1 DSGVO geeignete Maßnahmen treffen, um den Informations- und Mitteilungspflichten nach Art. 13 und 14 DSGVO Rechnung tragen und die entsprechenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln zu können.

Zur Umsetzung der Transparenz der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- Dokumentation der Mandanten und zugehörigen Datenbereiche
- Dokumentation von Auftrags- und Unterauftragsverhältnissen
- Bereitstellung der Informationen für Auskunftsersuchen betroffener Personen
- Dokumentation verbindlicher Löschfristen

2 Zweckbindung

Die DSGVO verfolgt das Ziel, das personenbezogene Daten ausschließlich für einen präzise definierten Zweck verarbeitet werden dürfen. Betroffene müssen im Sinne der Transparenz Auskunft über den Zweck einer Verarbeitung ihrer personenbezogenen Daten erhalten.

Zur Umsetzung der Zweckbindung in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Darstellung der Zwecke im Verzeichnis von Verarbeitungstätigkeiten
- Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DSGVO
- Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten, insbesondere im Rahmen von Teleheimarbeit (Home-Office)
- Entgegennehmen ausschließlich schriftlicher Weisungen nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers

3 Datenminimierung

Die DSGVO verfolgt das Ziel, dass Verantwortliche die Verarbeitung personenbezogener Daten auf den Umfang an Daten beschränken, der für die Umsetzung des Zwecks der Verarbeitung notwendig ist oder durch gesetzliche Bestimmungen gestattet sind.

Diese Form der Datenminimierung im Sinne des Art. 5 Abs. 1 lit. c DSGVO ist gewährleistet, wenn die Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung not-wendige Maß beschränkt sind.

Zur Umsetzung der Datenminimierung in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Datenschutz durch datenschutzfreundliche Gestaltung der Technik (Privacy-by-Design)
- Regelmäßig Prüfung der Beschränkung der Datenerhebungen gegen den jeweiligen Zweck und die Rechtsgrundlage der Verarbeitung
- Festlegung verbindlicher Löschfristen
- Umsetzung der verbildlichen Löschfristen durch regelmäßiges *manuelles* Löschen nicht benötigter Daten
- Umsetzung der verbildlichen Löschfristen durch regelmäßiges *automatisiertes* Löschen nicht benötigter Daten

4 Richtigkeit

Die DSGVO verfolgt das Ziel, dass Verantwortliche die Richtigkeit verarbeiteter personenbezogener Daten Betroffener umsetzen. Betroffene haben ein Recht auf die Richtigkeit ihrer Daten, die im Zeug der fortschreitenden automatisierten Vernetzung und maschinellen Auswertung von Daten aus unterschiedlichsten Quellen (Profiling im Big-Data) und angeschlossener automatisierter Entscheidungssysteme auf Basis von Techniken des maschinellen Lernens denen sich Betroffene ausgesetzt sehen, zunehmend an Bedeutung gewinnen wird.

Richtigkeit im Sinne des Art. 5 Abs. 1 lit. d DSGVO ist gewährleistet, wenn die verarbeiteten Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind und Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Zur Umsetzung der Richtigkeit in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Dokumentation zum Nachweis der Datenherkunft in der Robin Data Software
- Verwendung von Sicherheitszertifikaten zur Authentifizierung an Datenquellen
- Nutzung sicherer Datenübermittlungsverfahren die eine Manipulation versendeter Daten verhindern (über sicherer Cloud-Speicher, Verbindung zur App verschlüsselt)
- Nutzung von Identifikationsverfahren zur Richtigen Zuordnung von Person und angefragtem Datensatz (Session-Management)
- Unverzügliche Korrektur unrichtiger Daten bei Feststellung (Daten des Kunden liegen in seiner Verantwortung)
- Unverzügliche Löschung unrichtiger und nicht korrigierbarer Daten

5 Speicherbegrenzung

Die DSGVO verfolgt das Ziel, dass Verantwortliche personenbezogene Daten nur für die Dauer des definierten Zwecks, definierter gesetzlicher Aufbewahrungsfristen oder zur Umsetzung eines in engem Rahmen zu gestattenden berechtigten Interesses speichern und danach unverzüglich Löschen. In der Regel ist die Dauer der Speicherung personenbezogener Daten unmittelbar abhängig vom entsprechenden Datenverarbeitungsverfahren.

Speicherbegrenzung im Sinne des Art. 5 Abs. 1 lit. e DSGVO ist gewährleistet, wenn die verarbeiteten Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Ergänzend zu obigen Maßnahmen wird die Umsetzung der Speicherbegrenzung in der Verarbeitung von dem Verantwortlichen durch folgende Maßnahmen sichergestellt:

- Anonymisierte Meta-Auswertung von Nutzerstatistiken
- Umsetzung des Löschkonzeptes

6 Vertraulichkeit

Die DSGVO verfolgt das Ziel, dass Verantwortliche personenbezogene Daten derart verarbeiten, dass nur berechtigte Personen Zugriff auf dieses Daten erlangen. Die Sicherstellung der Vertraulichkeit ist zentrales ein Schutzziel der Daten- und Informationssicherheit.

Vertraulichkeit im Sinne des Art. 32 Abs 1 lit. b in Verbindung mit ErwGr 39 und 83 DSGVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem gemäß Art. 5 Abs. 1 lit. f DSGVO vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind.

Zur Umsetzung der Vertraulichkeit in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

In den Büroanlagen von Robin Data:

- Sicherheitstüren mit Transponderregelungen
- Wachdienst, mit Schließzeiten des Büros
- Putzdienst kommt während der Bürozeiten
- Besucherempfangsregelungen
- Schlüsselbuch
- Sicherung der Datenverarbeitungsanalagen

In den Rechenzentren der Unterauftragnehmer von Robin Data:

- Die Daten werden ausschließlich in ISO/IEC 27001 zertifizierten Rechenzentren verarbeitet

Im Zugang zur Robin Data Software und der von Robin Data genutzten Software zur Auftragserfüllung

- Umsetzung von Rollen- und Rechtemanagement:
- Arbeiten mit individuellen Benutzerkennungen
- Regelungen zur Sperrung von Zugängen ausscheidender Mitarbeiter
- Passwortrichtlinien (Durchsetzung, wenn möglich automatisiert)
- Authentifikation durch Verzeichnisdienste
- Kontensperrung bei mehrfacher falscher Authentifikation
- Benutzer sperren Rechner beim Verlassen des Arbeitsplatzes
- Automatisierte Abmeldung von Nutzern nach Time-Out
- Clean-Desktop-Philosophie umgesetzt
- Nutzung von Blickschutzfiltern auf mobilen Geräten in öffentlichen Räumen

Im Zugriff zur Robin Data Software und der von Robin Data genutzten Software zur Auftragserfüllung

- Minimierung von Administratorzugängen
- Aufteilung der Administratorrechte auf verschiedene Personen
- Zugriffrechte orientieren sich an Zuständigkeiten
- Zugriffrechte orientieren sich an Zuständigkeiten
- Einsatz von Datenträgerverschlüsselung
- Einsatz von Mailverschlüsselung
- Verschlüsselung mobiler Geräte (Laptops, Mobile Devices)
- Datenträgervernichtung nach DIN 66399
- Trennung von Test-und Produktivsystemen
- Logische Mandantentrennung
- Einsatz von VPN-Netzwerk

7 Integrität

Die DSGVO verfolgt das Ziel, dass Verantwortliche personenbezogene Daten derart verarbeiten, das diese Daten jederzeit korrekt verarbeitet werden und Veränderungen an den Daten nachvollzogen werden können (Revisionssicherheit).

Integrität im Sinne des Art. 32 Abs. 1 lit. b in Verbindung mit Art. 5 Abs. 1 lit. f DSGVO ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt10 sind

Zur Umsetzung der Integrität in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Signieren von E-Mails
- Einsetzen eines Secure-Mail-Gateway zur DSGVO-konformen Mailübertragung
- Verschlüsselung von Datenbanken
- Dokumentenmanagement mit Versionierungssystem
- Umsetzung der Vorgaben der GOBS/GOBD
- Einsatz von Virenschutzlösungen
- Dedizierte Netze entsprechend Schutzziele

- Update-und-Patch-Management
- Firewall im Büro
- Mehrstufige Firewall in der Robin Data App

8 Verfügbarkeit

Die DSGVO verfolgt das Ziel, dass Verantwortliche personenbezogene Daten derart verarbeiten, das diese Daten jederzeit auf Anfrage des Nutzers abrufbar sind. Dieses betrifft vor allem Dienste, die ihre Daten online erheben und zur Verfügung stellen.

Verfügbarkeit im Sinne des Art. 32 Abs. 1 lit. b DSGVO ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gemäß Art. 32 Abs. 1 lit. c DSGVO die Fähigkeit existieren die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

Zur Umsetzung der Integrität in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

- Datensicherungs-Konzept umgesetzt (Backup-Konzept mehrmals täglich, rollierend)
- Backup-Konzept getestet (Recovery-Test)
- Aufbewahrung sensibler Datenträger in sicheren Behältnissen
- Aufbewahrung der Datensicherung in einem anderen Brandabschnitt
- Festgelegt Zuständigkeiten im Rahmen der Datensicherung
- Einsatz von Virtualisierungslösungen
- Geo-Redundante Datenverarbeitung
- Notfallplan bei Betriebsproblemen umgesetzt
- Automatisierte Alarmsysteme bei Systemausfällen

9 Belastbarkeit

Die DSGVO verfolgt das Ziel, dass Verantwortliche personenbezogene Daten derart verarbeiten, das die verarbeitenden Systeme auch größten Belastungen, z. B. bei Hackerangriffen oder intensiver Benutzeraktivitäten, standhalten.

Belastbarkeit ist gemäß Art. 32 Abs. 1 lit. b auf Dauer sicherzustellen und betrifft Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Zur Umsetzung der Integrität in der Verarbeitung hat der Verantwortliche folgende Maßnahmen getroffen:

Lastenausgleich

- Cloud-basierter-Lastenausgleich (load balacing) durch Microservices
- Skalierung des Lastenausgleichs erfolgt automatisiert
- Skalierungslevel des Lastenausgleichs ist automatisiert limitiert

Absicherung der technischen Verfügbarkeit

- Die Daten werden ausschließlich in ISO/IEC 27001 zertifizierten Rechenzentren verarbeitet

10 Rechenschaftspflichten und Wirksamkeitsnachweis

Rechenschaftspflicht im Sinne des Art. 5 Abs. 2 DSGVO ist erfüllt, wenn der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen

kann. Unabhängig davon muss er gemäß Art. 32 Abs. 1 lit. d DSGVO in der Lage sein, die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüfen, bewerten und evaluieren zu können. Außerdem muss er gem. ErwGr 87 DSGVO sofort feststellen können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.

Zur Umsetzung der Rechenschaftspflichten und zum Nachweis der Wirksamkeit der Maßnahmen hat der der Verantwortliche folgende Maßnahmen getroffen:

- Führen des Verzeichnisses der Verarbeitungstätigkeiten (VV)
- Aufbau einer Datenschutzorganisation (mit oder ohne DSB)
- Dokumentation getroffener Sicherheitsmaßnahmen (VV, TOMs)
- Nachweis der Umsetzung des Rollen-/Rechtemanagements
- Regelmäßige Prüfung und Auswertung der Protokolle (KVP)
- Dokumentation der vorhandenen IT-Infrastruktur und der Schutzbedarfe (laufend)
- Bestellung eines Datenschutzbeauftragten (DSB)
- Protokollierung von Anmeldevorgängen und Zugriffen
- Protokollierung von Löschvorgängen / Entsorgungsvorgängen
- Protokollierung der Zutritts zu den Datenverarbeitungsanlagen im Rechenzentrum
- Protokollierung der Tätigkeiten der Systemadministratoren
- Dokumentation der Tätigkeiten der Datenschutzzuständigen
- Kontinuierliche Aktualisierung des Datenschutz-Management-Systems
- Regelmäßige dokumentierte Schulungen der Mitarbeiter auf den Datenschutz