Der vorliegende Datenverarbeitungsvertrag (der „Vertrag“) wird zwischen der **auf dem Bestellformular aufgeführten verantwortlichen Partei** (nachfolgend „Kunde“) und dem Auftragsverarbeiter, Ungerboeck Systems International GmbH, Kaiserstrasse 72, 76137 Karlsruhe, Deutschland (nachfolgend „Auftragnehmer“) abgeschlossen.

Präambel

Der vorliegende Vertrag legt die konkreten Datenschutzverpflichtungen der Vertragsparteien fest, die sich aus dem Vertragsverhältnis zwischen den Parteien ergeben, und wird hiermit in alle bestehenden und aktuellen Bestellformulare/Angebote/Leistungsvereinbarungen, einschließlich der Geschäftsbedingungen Rahmenlizenzvertrag, des Wartungsvertrags und/oder des Cloud-Hosting-Vertrags, aufgenommen; nachfolgend gemeinsam als „Leistungsvereinbarung“ bezeichnet.

Der vorliegende Vertrag gilt für alle Tätigkeiten, bei denen Mitarbeiter des Kunden oder vom Auftragnehmer beauftragte Personen personenbezogene Daten des Kunden verarbeiten. Um sicherzustellen, dass die geltenden Datenschutzgesetze hinsichtlich der Übermittlung personenbezogener Daten von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter innerhalb des Europäischen Wirtschaftsraums („EWR“), der Schweiz oder des Vereinigten Königreichs („UK“) an einen Auftragsverarbeiter außerhalb des EWR, der Schweiz oder der UK befolgt werden, und um die Gesetzesänderungen in Europa, der Schweiz und der UK nach der Genehmigung der neuen Standardvertragsklauseln durch die Europäische Kommission und des Zusatzes für die UK durch das Information Commissioner's Office der UK zu berücksichtigen, ändern die Parteien hiermit ihre im Vertrag festgelegten Datenübertragungsmechanismen wie folgt:

1. Gegenstand und Dauer des Auftrags/Vertrags

(1) Vertragsgegenstand

Der Gegenstand des Auftrags ist in der Leistungsvereinbarung definiert.

(2) Dauer

Die Dauer des Auftrags (Laufzeit der Auftragsabwicklung) entspricht der Laufzeit der entsprechenden Leistungsvereinbarung.

2. Spezifikation des Vertragsgegenstandes

(1) Art und Zweck der beabsichtigten Datenverarbeitung

Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Kunden sind in der Leistungsvereinbarung ausdrücklich dargelegt. Dies sind insbesondere:

- Cloud-Dienste (Hosting) der Datenbank für die Nutzung der Softwarelösung
- Verarbeitung von in Datenbanken gespeicherten Daten zugehöriger Webserver durch den Auftragnehmer zur Durchführung von Support, Wartung und Weiterentwicklung (z. B. Support-Tickets, Fehlerbehebung, Betriebsunterstützung, Remote-Meetings (GoToMeeting) usw.)
- Verarbeitung personenbezogener Daten für die Übertragung von Rechten (ausschließlich für die Webserver) nach Beauftragung durch den Kunden.
- Zugriff auf Protokolldateien zur Fehlererkennung und -behebung.
- Implementierung von Import-, Export- und Migrationsprozessen, einschließlich personenbezogener Daten (technischer und operativer Support).
- Entwicklung und Implementierung von Schnittstellen für die Datenübertragung zwischen Systemen.

(2) Art der Daten

Die Verarbeitung personenbezogener Daten schließt die folgenden Arten/Kategorien von Daten ein:

- Personenstammdaten, z.B. Vorname, Nachname, Anrede/Geschlecht, akademischer Titel, Abteilung/Position

- Kommunikationsdaten, z. B. Telefonnummer, E-Mail-Adresse, Fax-Nr., Mobilnummer
- Vertragsstammdaten, z.B. Vertragsverhältnis, Produkt oder Vertragsinteresse, Marktsegment
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Kontrolldaten
- Berechtigungen und Systemzugriffsrechte
- Passwörter
- Statistische Daten
- Benutzeraktivitäten (Protokolldateien/Log files)
- Vom Web-Benutzer eingegebene Daten
- IP-Adressen der Benutzer

(3) Kategorien von betroffenen Personen

Zu den Kategorien von Personen, die von der Verarbeitung betroffen sind, gehören:

- Benutzer der Webportale des Kunden (z. B. Interessenten, Kunden, Vertragspartner, Ansprechpartner, Kontaktpersonen)
- Kunden
- Interessenten und potenzielle Interessenten
- Abonnenten
- Vertragspartner
- Beschäftigte
- Lieferanten
- Kontaktpersonen

3. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Kunden zur Befolgung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der geltenden Vorschriften zum Schutz personenbezogener Daten erforderlich sind. Dazu gehören insbesondere die Anforderungen von Art. 32 der DSGVO. Der Auftragnehmer verpflichtet sich außerdem, seine Verpflichtungen gemäß Art. 32(1)(d) der DSGVO, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.

(2) Der Auftragnehmer sorgt für die Sicherheit gemäß Art. 28 (3) c), 32 der Datenschutz-Grundverordnung, insbesondere in Verbindung mit Art. 5 (1), (2) der DSGVO. Grundsätzlich handelt es sich bei den zu treffenden Maßnahmen um Datensicherheitsmaßnahmen und um die Gewährleistung eines dem Risiko angemessenen Schutzniveaus in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und die Belastbarkeit der Systeme. Dabei ist der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 (1) der DSGVO zu berücksichtigen.

(3) Der Stand der technischen und organisatorischen Maßnahmen, die zum Zeitpunkt des Abschlusses der Leistungsvereinbarungs bestehen, ist als **Anlage 1** beigefügt.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der weiteren Entwicklung. Es ist dem Auftragnehmer diesbezüglich gestattet, alternative angemessene Maßnahmen zu ergreifen. Hierbei darf das Sicherheitsniveau der angegebenen Maßnahmen jedoch nicht unterschritten werden. Wesentliche Änderungen müssen dokumentiert werden. Der Kunde kann jederzeit eine aktuelle Version der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die personenbezogenen Daten nur verarbeiten, (i) soweit dies für die Erbringung der Leistung erforderlich ist, (ii) in Übereinstimmung mit den spezifischen Anweisungen, die er vom Kunden erhalten hat, einschließlich in Bezug auf etwaige Übertragungen, und (iii) soweit dies zur Einhaltung von Gesetzen erforderlich ist (in diesem Fall wird der Auftragnehmer den Kunden vorab über eine solche gesetzliche Anforderung informieren, es sei denn, das Gesetz verbietet diese Offenlegung).

(2) Soweit im Leistungsumfang enthalten, werden das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung, die Datenübertragbarkeit und die Auskunft nach dokumentierten Weisungen des Kunden direkt durch den Auftragnehmer sichergestellt.

5. Qualitätssicherung und andere Verpflichtungen des Auftragnehmers

Neben der Befolgung der Bestimmungen in diesem Auftrag hat der Auftragnehmer gesetzliche Verpflichtungen gemäß Art. 28 bis 33 der DSGVO; dabei hat der Auftragnehmer insbesondere die Einhaltung der folgenden Anforderungen sicherzustellen:

- Schriftliche Ernennung eines Datenschutzbeauftragten, der seine Aufgaben gemäß Art. 38 und 39 der DSGVO ausübt. Die Kontaktdaten des externen Datenschutzbeauftragten können jederzeit auf der Website des Auftragnehmers unter https://ungerboeck.com/privacy-policy aufgerufen werden, die von Zeit zu Zeit geändert werden kann.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Ziff. B, 29, 32 Abs. 4 der DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die zur Verschwiegenheit verpflichtet und vorab mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht wurden. Der Auftragnehmer und ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich gemäß den Anweisungen des Kunden verarbeiten, einschließlich der in diesem Vertrag erteilten Befugnisse, es sei denn, sie sind gesetzlich zur Verarbeitung dieser Daten verpflichtet.
- Die Durchführung und Befolgung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 Ziff. C, 32 der DSGVO (siehe Anhang 1).
- Die Teilnahme an Anfragen der Aufsichtsbehörde an den Kunden, soweit sie diese Auftragsverarbeitung betreffen.
- Die unverzügliche Unterrichtung des Kunden über Kontrollaktionen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde gegen den Auftragnehmer im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens im Hinblick auf die Verarbeitung personenbezogener Daten bei der Auftragsabwicklung ermittelt.
- Sofern der Kunden einer Prüfung durch die Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, Haftungsansprüchen einer betroffenen Person oder eines Dritten oder sonstigen Ansprüchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, wird der Auftragnehmer den Kunden nach besten Kräften unterstützen.
- Der Auftragnehmer überwacht regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung in seinem Verantwortungsbereich in Übereinstimmung mit den Anforderungen des geltenden Datenschutzrechts erfolgt und dass der Schutz der Rechte der betroffenen Person gewährleistet ist.
- Die Überprüfbarkeit der technischen und organisatorischen Maßnahmen, die gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse gemäß Abschnitt 7 dieses Vertrags getroffen werden.

6. Beziehungen zwischen Unterauftragsverarbeitern

(1) Als Unterauftragsverarbeiter im Sinne dieser Bestimmung gelten diejenigen Leistungen, die sich direkt auf die Erbringung der Hauptdienstleistung beziehen. Ausgenommen hiervon sind Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsdienste, Post-/Transportdienste, Wartungs- und Benutzerservice oder die Entsorgung von Datenträgern in Anspruch nimmt, sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungssystemen. Der Auftragnehmer ist allerdings verpflichtet, auch bei ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden durchzuführen.

(2) Der Auftragnehmer kann insbesondere die Dienste von verbundenen Unternehmen oder anderen Anbietern als Unterauftragsverarbeiter nutzen, um seine Verpflichtungen aus diesem Vertrag zu erfüllen. Der Auftragnehmer führt eine aktuelle Liste der im Rahmen der Leistungen eingesetzten

Unterauftragsverarbeiter, einschließlich des Namens des Unterauftragsverarbeiters und des Zwecks seiner Verarbeitung. Der Kunde kann Benachrichtigungen über neue Unterauftragsverarbeiter erhalten, indem er eine E-Mail mit dem Betreff „Abonnieren“ an privacy@ungerboeck.com sendet. Sobald er sich auf diese Weise angemeldet hat, wird der Kunde über neue Unterauftragsverarbeiter benachrichtigt, bevor diese Unterauftragsverarbeiter berechtigt sind, personenbezogene Daten im Namen des Auftragnehmers zu verarbeiten. Der Kunde kann in angemessener Weise gegen die Nutzung eines neuen Unterauftragsverarbeiters durch den Auftragnehmer Einspruch erheben, indem er den Auftragnehmer innerhalb von 14 Tagen nach Erhalt der Benachrichtigung über die beabsichtigte Beauftragung schriftlich über privacy@ungerboeck.com informiert. Die angemessenen Gründe für einen Widerspruch sind in dieser Mitteilung zu erläutern (z. B. wenn die Nutzung dieses Unterauftragsverarbeiters gegen geltende Gesetze verstoßen oder den Schutz der betreffenden personenbezogenen Daten schwächen würde). Der Auftragnehmer wird sich in wirtschaftlich vertretbarem Umfang bemühen, den Einwand des Kunden zu beseitigen.

(3) Der Auftragnehmer darf ohne vorherige Zustimmung des Kunden keine personenbezogenen Daten übermitteln (und seinen Unterauftragsverarbeitern die Übermittlung von personenbezogenen Daten nicht gestatten). Der Auftragnehmer ist sich dessen bewusst, dass der Kunde zustimmen und dokumentieren muss, dass nach der Übermittlung ein angemessener Schutz der personenbezogenen Daten besteht, indem er Verträge verwendet, die ausreichende Garantien bieten (z. B. Standardvertragsklauseln), sofern keine andere Rechtsgrundlage für die Übermittlung besteht. Der Kunde stimmt hiermit der Übermittlung von personenbezogenen Daten durch den Auftragnehmer an die in diesem Abschnitt 6 beschriebenen Unterauftragsverarbeiter zu. Des Weiteren nimmt der Kunde zur Kenntnis und erklärt sich damit einverstanden, dass der Auftragnehmer (und seine Unterauftragsverarbeiter) in den Vereinigten Staaten, dem Vereinigten Königreich, Australien, Neuseeland oder Indien ansässig ist und der Auftragnehmer (und die Unterauftragsverarbeiter) Leistungen von diesen Ländern aus erbringen. Der Kunde willigt hiermit in die Übermittlung personenbezogener Daten in diese Länder zur Verarbeitung durch den Auftragnehmer und seine Unterauftragsverarbeiter gemäß des vorliegenden Vertrags ein. Der Kunde genehmigt hiermit die Beauftragung der in **Anlage 2** aufgeführten Unterauftragsverarbeiter.

7. Kontrollrechte des Kunden

(1) Der Kunde hat das Recht, in Absprache mit dem Auftragnehmer Inspektionen durchzuführen oder durch im Einzelfall zu benennende Inspektoren per E-Mail an privacy@ungerboeck.com durchführen zu lassen.

(2) Nach Erhalt der Aufforderung besprechen und vereinbaren die Parteien im Voraus den angemessenen Umfang, den Starttermin und die Dauer dieser Prüfung sowie alle erforderlichen Sicherheits- und Vertraulichkeitskontrollen. Der Auftragnehmer kann eine Gebühr (auf der Grundlage der angemessenen Kosten des Auftragnehmers) für eine solche Revision erheben. Der Auftragnehmer wird dem Kunden vor der Revision weitere Einzelheiten zu dieser Gebühr, einschließlich der Berechnungsgrundlage, mitteilen. Weiterhin ist der Kunde für alle Gebühren verantwortlich, die von einem vom Kunden für diese Prüfung beauftragten Drittprüfer erhoben werden.

8. Meldung von Verstößen durch den Auftragnehmer

(1) Der Auftragnehmer unterstützt den Kunden bei der Befolgung der in den Artikeln 32 bis 36 der DSGVO festgelegten Verpflichtungen in Bezug auf die Sicherheit personenbezogener Daten, die Meldepflichten bei Datenschutzverletzungen, die Datenschutz-Folgenabschätzung und die vorherige Konsultation. Hierzu gehören unter anderem:

a) die Gewährleistung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die den Umständen und Zwecken der Verarbeitung sowie der voraussichtlichen Wahrscheinlichkeit und Schwere einer potenziellen Sicherheitsverletzung Rechnung tragen und eine rasche Aufdeckung relevanter Sicherheitsverletzungen ermöglichen
b) die Verpflichtung, Verstöße gegen personenbezogene Daten dem Kunden unverzüglich zu melden
c) Die Verpflichtung, den Kunden bei der Erfüllung seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihr in diesem Zusammenhang alle relevanten Informationen ohne unangemessene Verzögerung zukommen zu lassen
d) Die Unterstützung des Kunden bei seiner Datenschutz-Folgenabschätzung
e) Die Unterstützung des Kunden im Rahmen der vorherigen Absprache mit der zuständigen Aufsichtsbehörde.

(2) Der Auftragnehmer kann eine angemessene Vergütung für Unterstützungsleistungen verlangen, die nicht in der Leistungsbeschreibung enthalten sind oder die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind.

9. Weisungsbefugnis des Kunden

(1) Der Kunde hat das Recht, dem Auftragnehmer jederzeit Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Anweisungen des Kunden werden zu Beginn in der Leistungsvereinbarung festgelegt und können danach von den Parteien in einem Nachtrag geändert, ergänzt oder ersetzt werden.

(2) Regelungen über eine etwaige Vergütung von Mehraufwendungen, die dem Auftragnehmer aufgrund von nachträglichen Weisungen des Kunden entstehen, bleiben unberührt.

(3) Der Auftragnehmer wird den Kunden unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt oder nicht eingehalten werden kann. Der Auftragnehmer ist berechtigt, die Implementierung der jeweiligen Anweisung auszusetzen, bis sie vom Kunden bestätigt oder geändert wird, oder der Kunde kann die Übermittlung personenbezogener Daten an den Auftragnehmer aussetzen und/oder (sofern anwendbar) die Leistungsvereinbarung mit dem Auftragnehmer kündigen (gemäß den Bedingungen der Leistungsvereinbarung).

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Vervielfältigungen der Daten dürfen nicht ohne Wissen des Kunden angefertigt werden. Ausgenommen hiervon sind Sicherungskopien, falls diese für eine ordnungsgemäße Datenverarbeitung erforderlich sind, sowie Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt werden.

(2) Nach der Fertigstellung der vertraglich vereinbarten Arbeiten oder auf Verlangen des Kunden früher - jedoch spätestens bei Beendigung der Leistungsvereinbarung - wird der Auftragnehmer sämtliche Unterlagen, die in seinen Besitz gelangt sind, erstellte Bearbeitungs- und Verwertungsergebnisse sowie Dateien, die sich auf das Vertragsverhältnis beziehen, an den Kunden herausgeben oder nach vorheriger Zustimmung des Kunden entsprechend den datenschutzrechtlichen Anforderungen vernichten.

(3) Die Dokumentation, die dem Nachweis der ordnungsgemäßen Datenverarbeitung gemäß diesem Vertrag dient, wird vom Auftragnehmer über das Ende der Leistungsvereinbarung hinaus entsprechend der jeweiligen Aufbewahrungsfristen aufbewahrt. Der Auftragnehmer kann sie bei Beendigung der Leistungsvereinbarung zu seiner Entlastung an den Kunden übergeben.

(4) Der Auftragnehmer darf personenbezogene Daten, die im Rahmen des Auftrags verarbeitet werden, über die Beendigung der Leistungsvereinbarung hinaus speichern, wenn und soweit der Auftragnehmer zur Aufbewahrung der Daten gesetzlich verpflichtet ist. In solchen Fällen dürfen die Daten nur zum Zweck der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht müssen die Daten unverzüglich gelöscht werden und dem Kunden auf Wunsch bestätigt werden, dass dies geschehen ist.

11. EU SCCS UND UK ADDENDUM

(1) Sofern der Auftragnehmer personenbezogene Daten aus dem EWR, der Schweiz oder dem Vereinigten Königreich in einem Land außerhalb des EWR, der Schweiz oder des Vereinigten Königreichs verarbeitet, das keine Angemessenheitsentscheidung der zuständigen Behörden erhalten hat, erfolgt die Übermittlung auf der Grundlage der EU SCCs und/oder des UK Addendums, je nach Anwendbarkeit. Falls die EU SCCs und/oder das UK Addendum nicht anwendbar ist/sind, vereinbaren die Parteien, in gutem Glauben und ohne unnötige Verzögerung an der Umsetzung eines geeigneten alternativen Übermittlungsmechanismus zu arbeiten, der gemäß den anwendbaren Datenschutzgesetzen zulässig ist.

(2) Sofern der Auftragnehmer personenbezogene Daten, die unter die EU-Datenschutzgesetze, das DSG und/oder die Datenschutzgesetze des Vereinigten Königreichs fallen, in einem Land verarbeitet, das keinen Angemessenheitsentscheidung der Europäischen Kommission bzw. der schweizerischen oder britischen Behörden erhalten hat, nehmen die Parteien hiermit die EU SCC (für personenbezogene Daten, die unter die EU-Datenschutzgesetze bzw. das DSG fallen) und den britischen Nachtrag (für personenbezogene Daten, die unter die britischen Datenschutzgesetze fallen) durch Bezugnahme auf.

(3) Sofern die EU-SCCs Anwendung finden, gelten sie folgendermaßen als erfüllt:

- Wenn der Kunde ein für die Verarbeitung personenbezogener Daten Verantwortlicher und der Auftragnehmer ein für die Verarbeitung personenbezogener Daten Verantwortlicher (Auftragsverarbeiter) ist, gilt Modul 2 (Übermittlung von Verantwortlichen an Auftragsverarbeiter) als erfüllt, wenn:
    - Klausel 7 der EU SCCs, die „Kopplungsklausel (optional)“ als aufgenommen gilt;
    - in Klausel 9(a) der EU SCCs die Parteien Option 2, „Allgemeine schriftliche Vollmacht“, mit einer Frist von vierzehn (14) Tagen auswählen;
    - die optionale Formulierung in Klausel 11 der EU SCCs als nicht anwendbar gilt;
    - in Ziffer 12 alle Ansprüche, die im Rahmen der EU-SCCs geltend gemacht werden, den in der Leistungsvereinbarung dargelegten Bestimmungen und Bedingungen unterliegen. In keinem Fall darf eine Partei ihre Haftung in Bezug auf die Rechte der betroffenen Person gemäß den EU-SCCs einschränken;
    - in Klausel 17 der EU SCCs der Datenexporteur und der Datenimporteur vereinbaren, dass die EU SCCs dem Recht der Bundesrepublik Deutschland unterliegen und zu diesem Zweck Option 1 wählen;
    - in Ziffer 18 der EU SCCs der Datenexporteur und der Datenimporteur vereinbaren, dass alle Streitigkeiten von den Gerichten der Bundesrepublik Deutschland entschieden werden sollen;
    - die Anhänge I.A, I.B, II und III der EU SCC als durch die Angaben in Anhang I und Anhang II des vorliegenden Vertrags, deren Inhalt hiermit von den Parteien vereinbart wird, als ergänzt gelten; und
    - für die Zwecke des Anhangs I.C der EU SCCs die zuständige Aufsichtsbehörde die Aufsichtsbehörde des Landes ist, in dem der Datenexporteur seine Niederlassung hat. Wenn der Datenexporteur nicht im EWR ansässig ist, die Verarbeitung aber der DSGVO unterliegt, ist die zuständige Behörde die Aufsichtsbehörde der Bundesrepublik Deutschland.

(4) Soweit die Übermittlung personenbezogener Daten dem DSG unterliegt, gilt Folgendes:

- Verweise auf die DSGVO sind als Verweise auf das DSG und, sobald es in Kraft tritt, auf das überarbeitete DSG zu verstehen, sofern die Übermittlung personenbezogener Daten dem DSG/dem überarbeiteten DSG unterliegt.
- Der Begriff „Mitgliedstaat“, wie er in den genehmigten EU SCCS verwendet wird, darf nicht derart ausgelegt werden, dass er betroffene Personen in der Schweiz daran hindert, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Klausel 18(c) der EU SCCs einzuklagen. In Fällen, in denen das DSG Anwendung auf die Verarbeitung findet, schützen die EU SCCs auch die Daten von juristischen Personen bis zum Inkrafttreten des überarbeiteten DSG (die am 25. September 2020 in Kraft getretene Fassung, in der geänderten Fassung).
- Sofern der Kunde der Datenexporteur ist und die übermittelten personenbezogenen Daten ausschließlich dem DSG unterliegen, ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (der „EDÖB“) die zuständige Aufsichtsbehörde für die Zwecke von Anhang I.C der EU SCCs. Sofern die übermittelten personenbezogenen Daten sowohl dem DSG als auch der DSGVO unterliegen, sollte eine parallele Aufsicht gelten: Für das (revidierte) DSG ist der EDÖB die zuständige Aufsichtsbehörde, sofern die Übermittlung unter das (revidierte) DSG fällt; und für die DSGVO ist die zuständige Aufsichtsbehörde (a) die Aufsichtsbehörde des Landes, in dem der Datenexporteur niedergelassen ist, wenn der Datenexporteur im EWR niedergelassen ist, oder (b) die Aufsichtsbehörde von Irland, wenn der Datenexporteur nicht im EWR niedergelassen ist.

(5) Wenn das UK Addendum Anwendung findet, gilt er als abgeschlossen, wenn das Folgende vorliegt:

- Tabelle 1 gilt als durch die Angaben in Anhang I des vorliegenden Nachtrags ergänzt, dessen Inhalt hiermit von den Parteien vereinbart wird;
- In Tabelle 2 wählen die Parteien das Kontrollkästchen aus, das lautet: „Genehmigte EU-SCCs, einschließlich der Informationen im Anhang und mit nur den folgenden Modulen, Klauseln oder optionalen Bestimmungen der Genehmigten EU-SCCs, die für die Zwecke dieses Nachtrags in Kraft gesetzt werden“, und die beigefügte Tabelle gilt als entsprechend den in Ziffer 11.4 dargelegten Präferenzen der Parteien ausgefüllt. Für die Zwecke von Klausel 9 des UK Addendums gilt als anwendbares Recht das Recht von England und Wales
- Tabelle 3 gilt als durch die Angaben in Anhang I und Anhang II des vorliegenden Nachtrags ergänzt, deren Inhalt hiermit von den Parteien vereinbart wird;
- In Tabelle 4 vereinbaren die Parteien, dass jede Partei den Nachtrag gemäß Abschnitt 19 des UK Addendums kündigen kann.

(6) Zur Vermeidung von Missverständnissen gelten diese EU SCCs/UK Addendum unabhängig voneinander für alle verbundenen Unternehmen des Kunden im EWR und im Vereinigten Königreich (wo Klausel 1.6 gilt), die die vom Auftragnehmer erbrachten Leistungen nutzen können (wie im Anhang zu diesen EU SCCs definiert, die in diesen Vertrag aufgenommen wurden). Im Rahmen des EU SCCs/UK Addendum gelten die vorgenannten verbundenen Unternehmen des Kunden aus dem EWR und dem Vereinigten Königreich (sofern Klausel 11(5) Anwendung findet) jeweils als Datenexporteur und der Auftragnehmer als Datenimporteur.

12. Veränderungen der Richtlinien

(1) Der Auftragnehmer wird alle Änderungen am Vertrag (einschließlich der Gründe, die die Änderungen rechtfertigen) oder an der Liste der durch den Vertrag gebundenen Gruppenmitglieder mitteilen:

- den durch den Vertrag gebundenen Gruppenmitgliedern des Auftragnehmers, durch schriftliche Mitteilung (per E-Mail oder durch Veröffentlichung in einem internen Intranet, das allen Gruppenmitgliedern zugänglich ist); und
- dem Kunden und den Personen, die von dem Vertrag profitieren, durch Online-Veröffentlichung auf der Website des Auftragnehmers mitzuteilen (und wenn die Änderungen wesentlicher Natur sind, muss der Auftragnehmer dem Kunden die wesentlichen Änderungen auch aktiv mitteilen, bevor sie in Kraft treten, gemäß Absatz 12.2 unten).

(2) Wenn der Auftragnehmer wesentliche Änderungen am Vertrag oder an der Liste der durch den Vertrag gebundenen Gruppenmitglieder vornimmt, die sich auf das durch den Vertrag gebotene Schutzniveau auswirken oder den Vertrag anderweitig wesentlich beeinflussen, wird der Auftragnehmer diese Änderungen (einschließlich der Gründe, die diese Änderungen rechtfertigen) unverzüglich allen anderen Gruppenmitgliedern des Auftragnehmers mitteilen. Wenn eine vorgeschlagene Änderung des Vertrags wesentliche Auswirkungen auf die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag eines Kunden hat, wird der Auftragnehmer zudem:

- dem betroffenen Kunden die vorgeschlagene Änderung aktiv mitteilen, bevor sie in Kraft tritt, und zwar mit einer Frist von mindestens 14 Tagen, um dem betroffenen Kunden die Möglichkeit zu geben, Einwände zu erheben; und
- der Kunde kann in einem solchen Fall die Übermittlung personenbezogener Daten an den Auftragnehmer aussetzen und/oder gegebenenfalls die Leistungsvereinbarung gemäß der darin festgelegten Bedingungen mit dem Auftragnehmer kündigen.

13. Definitionen

(1) Anwendbare Datenschutzgesetze: bezeichnet das/die folgende(n) Datenschutzgesetz(e), soweit diese anwendbar sind, einschließlich aller nachfolgenden Ergänzungen, Änderungen und Überarbeitungen: (i) die EU-Verordnung 2016/679 mit dem Titel „Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („DSGVO“) und alle anwendbaren nationalen Gesetze, die von EWR-Mitgliedsländern umgesetzt werden“; (ii) das Schweizer Bundesgesetz vom 19. Juni 1992 über den Datenschutz (in seiner geänderten oder ersetzten Fassung); und (iii) das Datenschutzgesetz 2018 (c. 12) des Vereinigten Königreichs.

(2) EU-Datenschutzgesetze: bezeichnet die Rechtsvorschriften der Europäischen Union („EU“) zum Schutz der betroffenen Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, insbesondere die DSGVO (zusammen mit den zugehörigen nationalen Rechtsvorschriften) und die Richtlinie 2002/58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung, die von Zeit zu Zeit weiter geändert oder ersetzt werden kann, in den Ländern, die Mitglieder der EU oder des EWR sind, und andere Datenschutzgesetze (einschließlich im Wesentlichen ähnlicher Gesetze, die die DSGVO oder damit verbundene nationale Gesetze ersetzen), die von Zeit zu Zeit in den Ländern, die Mitglieder der EU oder des EWR sind, in Kraft sind.

(3) EU SCCs: bezeichnet die von der Europäischen Kommission jeweils genehmigten Standardvertragsklauseln für die Übermittlung personenbezogener Daten an für die Verarbeitung Verantwortliche und Auftragsverarbeiter mit Sitz in Drittländern in Übereinstimmung mit dem anwendbaren Datenschutzrecht, die zum Zeitpunkt der Unterzeichnung dieses Vertrags geltende genehmigte Fassung ist diejenige, die im Beschluss 2021/914 der Europäischen Kommission vom 4 Juni 2021, wie diese Standardvertragsklauseln sind verfügbar sind unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en und können von der Europäischen Kommission von Zeit zu Zeit geändert oder ersetzt werden.

(4) DSG: bezeichnet das schweizerische Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1) und die Verordnungen SR 235.11 und SR 235.13 in der jeweils geltenden Fassung sowie, nach Inkrafttreten am 1. September 2023 (oder einem anderen vom schweizerischen Recht festgelegten Datum), die revidierte Fassung des DSG vom 25. September 2020 in der jeweils geltenden Fassung.

(5) Personenbezogene Daten: sind alle Informationen, die sich direkt oder indirekt auf eine identifizierte oder identifizierbare natürliche Person beziehen und die vom Auftragnehmer oder den Unterauftragsverarbeiter im Rahmen der Leistungsvereinbarung verarbeitet werden. Ohne die Allgemeingültigkeit des Vorstehenden einzuschränken, umfasst der Begriff „personenbezogene Daten“ unter anderem „persönliche Daten“, „persönliche Informationen“ und ähnliche Begriffe, wie sie in den anwendbaren Datenschutzgesetzen definiert sind, soweit diese Daten im Rahmen des Vertrags verarbeitet werden.

(6) Auftragsverarbeitergruppe: bezeichnet den Auftragnehmer und jedes Unternehmen, das den Auftragnehmer kontrolliert, von ihm kontrolliert wird oder unter gemeinsamer Kontrolle mit ihm steht.

(7) Dienstleistungen: bezeichnet die Funktionen, die der Auftragnehmer im Namen des Kunden gemäß der Leistungsvereinbarung ausführt.

(8) UK Addendum: bezeichnet den Nachtrag des Vereinigten Königreichs für den internationalen Datentransfer zu den Standardvertragsklauseln der EU-Kommission, abrufbar unter https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, in der vom Information Commissioner's Office des Vereinigten Königreichs, dem Parlament oder dem Secretary of State angenommenen, geänderten oder aktualisierten Fassung.

(9) Datenschutzgesetze des Vereinigten Königreichs: bezeichnet den Data Protection Act 2018 (DPA 2018) in seiner geänderten Fassung und die EU-Datenschutz-Grundverordnung (EU-DSGVO), die als UK-DSGVO in das britische Recht aufgenommen wurde, in ihrer geänderten Fassung, sowie alle anderen anwendbaren Datenschutzgesetze des Vereinigten Königreichs oder aufsichtsrechtliche Verhaltenskodizes oder andere Leitlinien, die von Zeit zu Zeit herausgegeben werden können.

(10) Alle anderen in Großbuchstaben geschriebenen Begriffe, die hier nicht definiert sind, haben die im Vertrag oder in den anwendbaren Datenschutzgesetzen festgelegte Bedeutung. Ein Verweis auf einen Begriff oder einen Abschnitt der anwendbaren Datenschutzgesetze bedeutet die jeweils gültige Fassung.

Die Parteien haben den vorliegenden Vertrag durch ihre ordnungsgemäß bevollmächtigten Vertreter mit Wirkung zum Datum der Leistungsvereinbarung vereinbart.

Anhang 1

Der vorliegende Anhang beschreibt die Arten von Daten, die von Datenexporteuren übermittelt werden, und die Zwecke, für die diese Daten von den Auftragsverarbeitern/Datenimporteuren verarbeitet werden dürfen. Der vorliegende Anhang unterliegt den Bestimmungen des Vertrags. Begriffe in Großbuchstaben, die in diesem Anhang nicht definiert sind, haben die Bedeutung, die ihnen im Hauptteil des Vertrages oder in den geltenden Datenschutzgesetzen zugewiesen wird.

Datenexporteur:

- Der Datenexporteur ist: Kunde, wie in der Leistungsvereinbarung angegeben.
- Name (vollständiger rechtlicher Name): Wie in der Leistungsvereinbarung angegeben.
- Handelsname (sofern abweichend): Wie in der Leistungsvereinbarung angegeben.
- Adresse: Wie in der Leistungsvereinbarung angegeben.
- Offizielle Registrierungsnummer (falls vorhanden) (Unternehmensnummer oder ähnliche Kennung): Wie in der Leistungsvereinbarung angegeben.
- Name, Position und Kontaktdaten der Kontaktperson: Wie in der Leistungsvereinbarung angegeben.
- Aktivitäten, die für die gemäß diesen Klauseln übertragenen Daten relevant sind: Wie in der Leistungsvereinbarung angegeben.
- Unterschrift und Datum: Ausgeführt am selben Tag des Vertrags, die an dem Tag als ausgeführt gilt, an dem sie durch Unterzeichnung mittels elektronischer Signatur (z.B. DocuSign) akzeptiert wird.
- Rolle (Verantwortlicher/Auftragsverarbeiter): Wenn der Kunde die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt, ist er ein Verantwortlicher; wenn der Kunde im Namen und auf Anweisung eines Verantwortlichen handelt, ist er ein Auftragsverarbeiter.

Datenimporteure:

- Der Datenimporteur ist: Ungerboeck Systems International GmbH oder wie anderweitig im Unterschriftsblock des Vertrags vorgesehen.
- Name (vollständiger rechtlicher Name): Ungerboeck Systems International GmbH
- Adresse: Kaiserstrasse 72, 76133 Karlsruhe, Germany
- Offizielle Registrierungsnummer (falls vorhanden) (Unternehmensnummer oder ähnliche Kennung): Wie in der Leistungsvereinbarung angegeben.
- Name, Position und Kontaktdaten der Kontaktperson:
    - Herr Casey Jessmon, Chief Information Security Officer und Datenschutzbeauftragter (Global); privacy@ungerboeck.com
    - Frau Dorothee Schaeufele, Datenschutzkoordinatorin (EMEA); privacy@ungerboeck.com
- Aktivitäten, die für die gemäß diesen Klauseln übertragenen Daten relevant sind: Verarbeitung gemäß diesem Vertrag, der Leistungsvereinbarung und gemäß den dokumentierten Anweisungen im Namen des Kunden.
- Unterschrift und Datum: Ausgeführt am selben Tag des Vertrags, die an dem Tag als ausgeführt gilt, an dem sie durch Unterzeichnung mittels elektronischer Signatur (z.B. DocuSign) akzeptiert wird.
- Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

Kategorien von betroffenen Personen. Dieser Abschnitt gilt als abgeschlossen, wie im Vertrag beschrieben.

Art der personenbezogenen Daten. Dieser Abschnitt gilt als abgeschlossen, wie im Vertrag beschrieben.

Sensible personenbezogene Daten. Dieser Abschnitt gilt als abgeschlossen, wie im Vertrag beschrieben.

Häufigkeit der Verarbeitung: Diese Art der Verarbeitung wird kontinuierlich erfolgen.

Art und Zweck der Verarbeitung: Der Auftragnehmer erhebt, verarbeitet und nutzt alle personenbezogenen Daten ausschließlich für den Zweck der Verarbeitung, wie im Vertrag festgelegt und gemäß den dokumentierten Anweisungen im Namen des Kunden.

Dauer. Die Dauer der Datenverarbeitung hängt von der Laufzeit der Leistungsvereinbarung ab.

Aufbewahrungsfrist. Die Aufbewahrungsfrist der personenbezogenen Daten gilt für die Dauer des Vertrags oder wie darin anderweitig beschrieben.

Unterauftragsverarbeiter. Dieser Abschnitt gilt als ausgefüllt, wie im Vertrag, Anhang II, beschrieben und von Zeit zu Zeit geändert.

Technisch-organisatorische Maßnahmen

Weitere Informationen zu den Sicherheitsmaßnahmen in der Ungerboeck Cloud-Umgebung finden Sie auf den folgenden Seiten. Weitere Informationen über den Datenschutz bei Ungerboeck Systems International GmbH finden Sie in unserer Datenschutzhinweise unter https://ungerboeck.com/privacy-policy. Weitere Informationen über die Sicherheitsmaßnahmen von Ungerboecks Cloud-Anbieter Amazon Web Services finden Sie auf der AWS-Website unter https://aws.amazon.com/de/compliance/gdpr-center/.

A. Technisch-organisatorische Maßnahmen an Ungerboeck-Standorten.

1. Vertraulichkeit (Art. 32 Abs. 1 Ziff. b DSGVO)

- Zutrittsverwaltung und -kontrolle
  - Der Haupteingang ist verschlossen. Die Zugangsberechtigen zu den Büroräumen sind entweder im Besitz einer Chipkarte oder eines Schlüssels. Zentrale Ausgabe von Karten oder Schlüsseln einschließlich Protokollierung.
  - Videoüberwachung am Haupteingang der Büroräumlichkeiten.
  - Schützenswerte Räume (z. B. der Serverraum) sind immer verschlossen. Nur Mitarbeiter, die den Zugang zu diesen Räumen für ihre beruflichen Aufgaben benötigen, haben Zugang zu diesen Räumen.
- Elektronische Zugangsverwaltung
  - Beim Zugriff auf das CRM-System identifizieren sich die Benutzer mit ihrer Benutzer-ID und ihrem Passwort.
  - Die verfügbare WiFi-Verbindung für das Büro ist passwortgeschützt.
  - Ein durch eine falsche Autorisierung zum System ausgelöster Fehlerzustand führt dazu, dass der Zugang zum System nach einer bestimmten Anzahl von Versuchen gesperrt wird.
  - Benutzer-IDs und Passwörter werden in Übereinstimmung mit den Ungerboeck-Passwortrichtlinien erstellt (Sonderzeichen, Mindestlänge und regelmäßige Passwortänderungen).
  - Es gibt Richtlinien für Mitarbeiter, die von zu Hause aus, mit mobilen Geräten oder vor Ort beim Kunden arbeiten.
  - Es gibt Sicherheitsrichtlinien und -konzepte für die unten beschriebenen Maßnahmen, die jährlich überprüft und aktualisiert werden.
- Trennungskontrolle
  - Ungerboeck folgt den Grundsätzen der Aufgabentrennung und dem Least-Privilege-Prinzip (so wenig Rechte wie möglich). Dies wird unter anderem mit Hilfe von Zugriffsanträgen und Überprüfungen durchgesetzt.
  - Die Entwicklungs- und Produktionsumgebungen sind voneinander getrennt, und die Berechtigungen werden pro Umgebung vergeben.
- Pseudonymisierung (Art. 32 Abs. 1 Ziff. a der DSGVO; Art. 25 Abs. 1 der DSGVO).
  - Die Pseudonymisierung für Kunden ist auf Anfrage im CRM-System möglich und wird bei Bedarf manuell durchgeführt. Andernfalls können die Daten gesperrt oder anonymisiert werden.
  - Wenn Ungerboeck aggregierte Daten für interne Zwecke verwendet, werden diese Informationen pseudonymisiert.
  - Für die unten beschriebenen Maßnahmen gibt es Sicherheitsrichtlinien und -konzepte, die jährlich überprüft und aktualisiert werden.

2. Integrität (Art. 32 Abs. 1 Ziff. b DSGVO)

- Übermittlungskontrolle

- Es gibt autorisierte Datenübermittlungsmethoden (MediaShuttle, SFTP). Die Verfahren sind dokumentiert.
- Die Anforderung und Übermittlung von Datenbankkopien wird in dem entsprechenden Support-Ticket festgehalten.
- Der Internetzugang ist durch VPN- und TSL/SSL-Verschlüsselungsmechanismen vor Abhörung geschützt. Die übermittelten Dateien werden regelmäßig und stichprobenartig auf ihre Integrität überprüft.
- E-Mails mit sehr sensiblen Informationen werden verschlüsselt (E-Mail-Verschlüsselung in Office 365).
- Es liegen Sicherheitsrichtlinien und -konzepte für die unten beschriebenen Maßnahmen vor, die jährlich überprüft und aktualisiert werden.

- Eingabekontrolle
  - Die Eingabe und Änderung von Stammdaten wird in Protokolldateien (Log files) im CRM-System aufgezeichnet.
  - Alle Datensätze werden zentral über ein unternehmensweites SIEM-Tool zusammengefasst.
  - Der Zugriff innerhalb des CRM-Systems wird durch eine benutzerdefinierte Konfiguration der Softwareeinstellungen (Benutzerrollen, Zugriffsrechte, Feldverschlüsselung oder -maskierung usw.) gesteuert.
  - Es liegen Sicherheitsrichtlinien und -konzepte für die unten beschriebenen Maßnahmen vor, die jährlich überprüft und aktualisiert werden.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Ziff. b DSGVO)

- Verfügbarkeitskontrolle
  - Ein Virenschutz auf dem neuesten Stand ist installiert. Firewall-Systeme sind im Einsatz.
  - Regelmäßige, stichprobenartige Integritätstests der Backups von lokalen Servern.
- Schnelle Wiederherstellbarkeit (Art. 32 Abs. 1 Ziff. c der DSGVO).
  - Das Konzept zur Sicherung der personenbezogenen Daten auf den lokalen Servern wurde implementiert.
  - Es besteht ein globaler Krisenplan („Global Disaster Recovery Plan“), der alle Büros und Rechenzentren abdeckt. RTOs und RPOs sind in unserem Business Continuity und Disaster Recovery Plan dokumentiert.
  - Es liegen Sicherheitsrichtlinien und -konzepte für die unten beschriebenen Maßnahmen vor, die jährlich überprüft und aktualisiert werden.

4. Verfahren zur regelmäßigen Überprüfung, Beurteilung und Bewertung (Art. 32 (1) (d) der DSGVO; Art. 25 (1) der DSGVO).

- Verwaltung des Schutzes personenbezogener Daten
  - Regelmäßige Datenschutzschulungen für die Mitarbeiter des Auftragnehmers
  - Regelmäßige Schulungen zur Cybersicherheit für die Mitarbeiter des Auftragnehmers
  - Ein internes Mitarbeiterhandbuch, das aus internen Datenschutz- und IT-Richtlinien zur Informationssicherheit und zu Datenschutzmaßnahmen in der EMEA-Organisation besteht, einschließlich Richtlinien für Mitarbeiter, die von zu Hause, mit mobilen Geräten oder vor Ort beim Kunden arbeiten.
  - Zusätzlich zu dem externen Datenschutzbeauftragten wurde ein interner Datenschutzkoordinator für die EMEA-Organisation ernannt.
  - Bildung eines globalen Datenschutzteams zur Stärkung der IT-Sicherheit und des unternehmensweiten Datenschutzmanagements.
- Management der Reaktion auf Vorfälle (Incident-Response-Management)
  - Der Plan zur Reaktion auf Vorfälle ist dokumentiert und wird mindestens einmal jährlich im Rahmen der BC/DR-Tests getestet und überprüft.

- Es besteht ein Team für die Reaktion auf Vorfälle, das sich seiner Verantwortung bewusst ist.
- Es liegen Sicherheitsleitlinien und -konzepte für die unten beschriebenen Maßnahmen vor, die jährlich überprüft und aktualisiert werden.

- Dem Schutz von personenbezogenen Daten dienende Standardeinstellungen (Art. 25 Abs. 2 DSGVO)
  - Ungerboeck Systems International GmbH unterstützt DSGVO-konforme Softwarelösungen durch „Datenschutz durch Technikdesign“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Ein adäquates Maß an Datenschutz kann durch die Einstellungen in der Softwarelösung und durch die individuelle Konfiguration der Einstellungen in Abhängigkeit von der jeweiligen Funktion erreicht werden (z. B. durch Zugriffsrechte, Feldverschlüsselung oder Feldmaskierung usw.).
- Vertragliche Verpflichtungen
  - Weitere Einzelheiten zu den vertraglichen Verpflichtungen sind in der Leistungsvereinbarung enthalten.
  - Weisungsgebundenheit, Mitteilungspflichten und Prüfungsrechte sind in dem vorliegenden Vertrag geregelt.
  - Die Mitarbeiter des Kunden, die dem Auftragnehmer Weisungen erteilen dürfen, werden von der Geschäftsführung des Kunden benannt.

B. Technisch-organisatorische Maßnahmen in den Ungerboeck Cloud-Umgebungen

Für die Cloud-Umgebungen nutzt Ungerboeck den branchenführenden Cloud-Anbieter Amazon Web Services („AWS“) für maximale Skalierbarkeit und Zuverlässigkeit der Cloud-Umgebungen sowie für Offsite-Backup und Katastrophenschutz (Disaster Recovery).

„Im Rahmen des AWS-Modells der geteilten Verantwortung bietet AWS eine globale, sichere Infrastruktur und grundlegende Rechen-, Speicher-, Netzwerk- und Datenbankservices sowie Services auf höherer Ebene. AWS bietet eine Reihe von Sicherheitsservices und -funktionen, die AWS-Kunden (Ungerboeck) nutzen können, um ihre Vermögenswerte zu schützen. AWS-Kunden (Ungerboeck) sind verantwortlich für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten in der Cloud und für die Erfüllung spezifischer geschäftlicher Anforderungen an den Informationsschutz.“
(Quelle: Amazon Web Services - Security Best Practices Whitepaper)

„Amazon Web Services (AWS) betreibt, verwaltet und kontrolliert die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen die AWS-Dienste betrieben werden. Der Kunde (Ungerboeck) ist für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches für das Gastbetriebssystem) und der zugehörigen Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Sicherheitsgruppen-Firewall und anderer sicherheitsrelevanter Funktionen verantwortlich.“
(Quelle: Amazon Web Services - EU Data Protection Whitepaper)

Bitte beachten Sie: Die nachfolgend beschriebenen Maßnahmen können sich je nach Verfügbarkeit der AWS-Services und dem Stand der Technik ändern. Die nachfolgende Auflistung enthält nicht die vollständigen technischen und organisatorischen Maßnahmen des Auftragnehmers, sondern soll dem Kunden lediglich einen Einblick in die getroffenen Maßnahmen geben. Weitere Einzelheiten über die Nutzung von Amazon Web Services durch Ungerboeck und die Sicherheitskontrollen sind auf Anfrage erhältlich.

1. AWS-Infrastruktur:
   - Weitere Informationen zu den Sicherheits- und Compliance-Maßnahmen des Cloud-Anbieters von Ungerboeck, Amazon Web Services, finden Sie auf der AWS Website.

2. Sicherheitsmaßnahmen in der Ungerboeck Cloud-Umgebung:
   - Die Datenbanken für EU-Kunden werden in der EU gehostet.
   - Ungerboeck setzt mehrere Schichten von Firewalls und Netzwerksicherheitstools ein, um die Datengrenzen zu schützen.
   - Alle öffentlich zugänglichen Zugangspunkte werden durch Zugriffskontrolllisten von den

Kernkomponenten isoliert. Nur die notwendigen Ports, die in gehostete Umgebungen ein- und ausgehen, sind offen.

- Der Anwendungszugriff wird durch die integrierte LDAP-Authentifizierung kontrolliert und alle Zugriffspunkte sind durch SSL/TSL-Verschlüsselung geschützt.
- Der Zugang über IP-Systeme wird nach einer bestimmten Zeit unterbrochen, wenn er nicht genutzt wird, dem so genannten Session-Timeout. Webserver-Sitzungen werden vom Server nach einer bestimmten Zeitspanne beendet.
- Auf allen Servern ist eine Antiviren- und Anti-Malware-Software installiert, die täglich aktualisiert und regelmäßig gescannt wird.
- Alle Server werden durch ein branchenführendes Intrusion Prevention System (IPS) geschützt, das den Netzwerkverkehr scannt und Methoden zur Erkennung bösartiger Dateien im Netzwerk identifiziert.
- Sensible Daten wie Passwörter und Kreditkarteninformationen in der Datenbank werden mit 256-Bit-AES und Split-Key-Verfahren verschlüsselt.
- Die Übertragung von Daten, die in die Anwendung ein- und ausgehen, ist durch TLS 1.2-Verschlüsselung oder höher geschützt.
- Kundendaten werden logisch getrennt und in einem nicht gemeinsam genutzten Datenbankschema und einer Anwendungsinstanz gesichert.
- Nicht genutzte Dienste und Anwendungen werden nach Möglichkeit entfernt oder deaktiviert.
- Die neuesten Sicherheitsupdates und Patches werden im Rahmen der regelmäßigen Wartung auf den Systemen installiert.
- Für den Zugriff auf die Verwaltungskonsolen ist eine Multi-Faktor-Authentifizierung erforderlich, sofern verfügbar.
- Der Zugriff auf Systemkomponenten und Daten ist auf Personen beschränkt, deren Aufgaben einen solchen Zugriff erfordern, sowie auf minimale Zugriffsprivilegien, die für die Durchführung der entsprechenden Aufgaben erforderlich sind.
- Ungerboeck hat komplexe Passwortrichtlinien implementiert, wie von der PCI-DSS-Compliance verlangt.
- Ungerboeck setzt vollständig verwaltete cloudbasierte Sicherheits- und Compliance-Dienste ein, um unerwünschte Sicherheitsverstöße zu überwachen, zu erkennen und umgehend darauf zu reagieren.
- Ungerboeck verfügt über eine 24x7 Log-Überwachung, -Analyse und -Prüfung, um Log-Daten von Cloud-, Server-, Anwendungs-, Sicherheits- und Netzwerk-Assets in der Ungerboeck-Cloud zu sammeln, zu aggregieren und zu durchsuchen.
- Ungerboeck setzt ein 24x7 vSOC ein, das eine kontinuierliche Überwachung aller Produktionssysteme durchführt.
- Ungerboeck stellt eine 24x7 Überwachung der Produktionssysteme unter Verwendung von Industriestandardverfahren, die das zuständige Personal von Ungerboeck über die Systemleistung und die Ressourcennutzung informieren.
- Ungerboeck verwendet eine Kombination von Technologien wie Load Balancing, Server Farming, Mirroring und Datenbankwartungspläne ein, um hohe Verfügbarkeit, Redundanz und Failover zu erreichen.

Anhang 2 - Unterauftragsverarbeiter

Unterauftragsverarbeiter / Land	Leistungen
Amazon Web Services, Inc. („AWS"), USA	Cloud-Services (Hosting) der Datenbank zur Nutzung der Softwarelösung sowie Testdatenbanken in der Cloud für Kunden mit entsprechendem Customer Success Plan. Nutzung von AWS-Rechenzentren in Europa.
Verbundene Unternehmen von Ungerboeck • Ungerboeck Systems International, LLC; USA und Neuseeland • Ungerboeck Software International, Pty Ltd.; Australien und Neuseeland • Olethia Pyt Ltd; Indien • Ungerboeck Systems International GmbH; United Kingdom	Support bei der Vertragsausführung: • Unterstützungsdienste (nach dem Prinzip „Follow-the-Sun") und technische Dienste; • Alpha/Beta/Early Adopter-Programm; • Web-Sitzungen und Online-Meetings; • Remote-Dienstleistungen oder Dienstleistungen vor Ort; • Technische Überwachung der Cloud-Umgebung (Verfügbarkeits- und Leistungsüberwachung sowie Fehlerbehebung im Falle einer Störung oder eines Ausfalls außerhalb der regulären Bürozeiten des Kunden); • Gilt nur für nicht gehostete Kunden (vor Ort): Für Support-Tests kann es erforderlich sein, mit den tatsächlichen Daten des Kunden zu testen, um einen Fehler reproduzieren zu können. Zu diesem Zweck wird der Kunde gebeten, eine Kopie seiner Datenbank über MediaShuttle bereitzustellen (alternativ kann der Kunde die Datenbankkopie auf den gesicherten EU-FTP-Server hochladen).
Zendesk, Inc., USA	Support Center und Wissensdatenban Ticket-System zur Bearbeitung von Support-Tickets für Ungerboeck-Software, Bereitstellung der Plattform, Server befinden sich in den USA.
LogMeIn, Inc., USA	GoToMeeting, GoToWebinar
NITOR Infotech Pvt. Ltd., Indien	Technische Entwicklungen, Qualitätstests
Altaa Vistaa Business Solutions Pvt Ltd, Indien	Customer Success Services, andere vertragliche Dienstleistungen (hauptsächlich, aber nicht ausschließlich, für englischsprachige Projekte eingesetzt)
OuiYou, Frankreich	Technische Schulungen und ähnliche Dienstleistungen für französischsprachige Kunden
Datajust B.V. (Storecove), Niederlande	Integration der elektronischen Rechnungsstellung in die Ungerboeck Software (PEPPOL) / Accesspoint als Dienstleistung
Stripe, Inc., USA	Nach dem Abonnement der vorgeschlagenen Dienste (Ungerboeck Payments / Payment Processing Services durch Ungerboeck Software)
Rossum Czech Republic s.r.o., Tschechische Republik	Nach dem Abonnement der vorgeschlagenen Dienstleistungen (Accounts Payable Automation durch Ungerboeck Software)
DocuSign Inc., USA	Nach der Subskription der vorgeschlagenen Dienstleistungen (Integration der elektronischen Signatur in die Ungerboeck Software einschließlich - falls zutreffend - der Bereitstellung von Umschlägen)
Jotform, Inc., USA	Bei der Anmeldung zu den vorgeschlagenen Dienstleistungen (Implementierung von Online-Formularen)
Twilio Inc., USA	Auf Wunsch des Kunden oder nach Genehmigung eines Angebots für eine individuelle Lösung (SendGrid Emails in Ungerboeck Software)
Signiant Inc., USA	Nutzung des MediaShuttle-Dienstes zum Hochladen und Übertragen von Datenbankkopien in die Ungerboeck Cloud-Umgebung; Nutzung durch Vor-Ort-Kunden auf Anfrage von Ungerboeck

Dynatrace, LLC, USA	Überwachungs- und Protokollierungsplattform eines Drittanbieters, die Ungerboeck zum Einlesen, Parsen, Abfragen und Analysieren von Ungerboeck-Anwendungen und Infrastrukturprotokollen verwendet.
Azure (Microsoft), USA	Cloud-Service-Provider für das Hosting von Shared-Services-Projekten im gesamten Produktportfolio von Ungerboeck.
Okta, Inc., USA	Identitätsanbieter
AC PM LLC (Postmark), USA	E-Mail-Dienstleister
Spreedly Inc., USA	Plattform für die Zahlungsabwicklung