Calenso

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach

EU-Datenschutz-Grundverordnung (DSGVO)

(AV-Vertrag)

Letzte Aktualisierung: 21.01.2026

1. Vereinbarung zur Auftragsverarbeitung

Die Vertragsparteien

Firma

Handelsregister-Nr.: Amtsgericht

– nachstehend bezeichnet als Auftraggeber –

und

Unternehmung	**Calenso AG**
Vorname / Name:	Marvin Felder
Funktion:	CEO
Strasse Nr.:	Sonnmatthof 3
PLZ, Ort, Land:	6023 Rothenburg, Schweiz
Handelsregister/Nr.:	CHE-360.668.485

– nachstehend bezeichnet als Auftragsverarbeiter –

schließen folgenden Vertrag:

1. Allgemeine Bestimmungen und Auftragsgegenstand

- Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind dem Anhang A zu entnehmen.
- Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für die Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.
- Die Verarbeitung der Daten durch den Auftragsverarbeiter findet grundsätzlich auf dem Gebiet der Schweiz, eines Mitgliedstaates der Europäischen Union oder eines Vertragsstaates des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) sowie Art. 32 DSGVO auch ohne vorherige Zustimmung des Auftraggebers.
- Die Vergütung wird außerhalb dieses Vertrags vereinbart. Alle in dieser Vereinbarung zur Auftragsverarbeitung genannten Leistungen sind durch die Vergütung der Hauptleistung abgegolten.
- Gerichtsstand ist der Sitz des Auftragsverarbeiters.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.
In Verbindung mit einem Calenso Abonnement ist die Gültigkeit des AV-Vertrages mit der Laufzeit des Abonnements verknüpft. Das Vertragsverhältnis beginnt mit dem Abschluss eines Calenso Abonnements bzw. mit der Nutzung des Dienstes. Mit Kündigung des Abonnements erlischt nicht die Gültigkeit des AV-Vertrags. Nach Kündigung eines Calenso Abonnements besteht die Option auf spätere Weiterführung des Abonnements. Personenbezogene Daten können dazu erhalten bleiben. Auf Wunsch des Auftraggebers können sämtliche Daten gelöscht und nicht weiter durch den Auftragsverarbeiter weiterverarbeitet werden. Mit dem Auftrag zur Löschung aller Daten erlischt die Gültigkeit des AV-Vertrags.

3. Weisungen des Auftraggebers

- Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung gegenüber dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen. Gesetzliche Interessen können z.B. buchhalterische bzw. Steuer-relevante Aufbewahrungsfristen oder strafrechtliche Ermittlungsverfahren sein.
- Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.
- Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.
- Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

- Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie in erforderlichem Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.
- Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen vor Ort Kontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.
- Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

- Der Auftragsverarbeiter verpflichtet sich explizit auf die Einhaltung der anwaltlichen Schweigepflicht, ärztlichen Schweigepflicht, sowie der Schweigepflichten aller genannten Berufsgruppen nach § 203 Abs. 1 Strafgesetzbuch (StGB) gegenüber dem Auftraggeber.

- Der Auftragsverarbeiter wurde vom Auftraggeber darüber belehrt, dass über sämtliche Daten von Mandantinnen und Mandanten absolute Verschwiegenheit über alle im Rahmen der Beauftragung bekannt gewordenen Vorgänge und Daten zu wahren ist. Die Pflicht zur Verschwiegenheit besteht gegenüber allen, insbesondere auch gegenüber Familienangehörigen der Mitarbeiterinnen und Mitarbeiter und gegenüber Subunternehmern. Es ist bekannt, dass die Verschwiegenheitsverpflichtung auch bei Beendigung der Geschäftsbeziehungen unverändert fortbesteht. Alle Personen und Subunternehmer, denen sich der Auftragsverarbeiter zur Erfüllung des Auftragsverhältnisses bedient, sind vor der Erbringung von Arbeiten vom Auftragsverarbeiter zur Verschwiegenheit im Sinne dieser Verschwiegenheitsverpflichtung zu verpflichten. Der Auftragsverarbeiter weist dem Auftraggeber diese Verpflichtung der Mitarbeiter sowie sonstiger Personen, denen er sich zur Erfüllung des Auftragsverhältnisses bedient, auf Verlangen nach. Es wird ausdrücklich darauf hingewiesen, dass eine Verletzung der Verschwiegenheitspflicht sowie das Unterlassen der Verschwiegenheitsverpflichtung weiterer Personen, derer sich der Auftragsverarbeiter zur Erfüllung des Auftragsverhältnisses bedient, Anlass zu einem Strafverfahren sein können. Die einschlägigen strafrechtlichen Vorschriften (§ 203 Abs.1, Abs.3, Abs. 4 StGB) sind bekannt. Ebenso ist bekannt, dass diese Vorschriften für den Auftragsverarbeiter und seine Mitarbeiterinnen und Mitarbeiter gelten. Es wird erklärt, dass die Belehrung verstanden wurde und keine weiteren Fragen und Aufklärungswünsche bestehen.

- Der Auftragsverarbeiter darf personenbezogene Daten von Mandantinnen und Mandanten (soweit diese von Anhang A umfasst sind) nur insoweit übermitteln, offenlegen oder bereitstellen, wie dies für die Inanspruchnahme der Tätigkeit der Mitarbeiterin, des Mitarbeiters oder des Subunternehmers erforderlich ist.

- Der Auftragsverarbeiter, seine Mitarbeiterinnen, Mitarbeiter und Subunternehmer dürfen sich nur insoweit Kenntnis von personenbezogenen Daten verschaffen, als dies für die Vertragserfüllung des Auftragsverarbeiters gegenüber dem Auftraggeber entsprechend der Regelungen des Hauptvertrages erforderlich ist.

- Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden) , wobei der Auftragsverarbeiter die Anforderungen von § 203 des Strafgesetzbuches zu beachten hat, auf das er in diesem Vertrag verpflichtet wird. Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.
- Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.
- Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

- Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind, in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist ohne Zustimmung des Auftraggebers gestattet. Die Einhaltung der Schutzmaßnahmen nach § 7 Absätzen 1 und 2 dieses Vertrags sowie der Maßgaben des Art. 32 DSGVO ist auch in diesem Fall sicherzustellen.
- Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Spezielle Verpflichtungen des Auftragsverarbeiters gegenüber Berufsgruppen mit besonderen Verschwiegenheitspflichten

- § 43e Bundesrechtsanwaltsordnung (BRAO) - Inanspruchnahme von Dienstleistungen
    - Der Auftragsverarbeiter ist über die strafrechtlichen Folgen einer Pflichtverletzung belehrt und zur Verschwiegenheit verpflichtet.
    - Der Auftragsverarbeiter ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.
    - Der Dienstleister ist befugt, weitere Personen zur Erfüllung des Vertrags heranzuziehen. Für diesen Fall ist es dem Dienstleister auferlegt, diese Personen in Textform zur Verschwiegenheit zu verpflichten.
    - Der bestehende Schutz der Geheimnisse ist für nicht in der Schweiz ansässige Auftraggeber mit dem Schutz in EU-Ländern vergleichbar.
    - Der Zugang zu fremden Geheimnissen von Mandanten gewährleistet der Auftraggeber dem Auftragsverarbeiter nur nach vorheriger Einwilligung des Mandanten. Dies ist technisch bereits in der Benutzeroberfläche umgesetzt.

.

7. Technische und organisatorische Maßnahmen

- Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese im Anhang B dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.
    - Art. 32 Abs. 1 Punkt a) DSGVO wird durch AES-Verschlüsselung der Endkundendaten erfüllt
    - Art. 32 Abs. 1 Punkte b),c) DSGVO: Folgende Punkte werden durch Verschlüsselung, redundanter Server-Standorte, Mitarbeiter-Zugriff mit 2-FA und Wiederherstellungs-Protokolle anhand genannter Redundanzen sichergestellt:
        - Fähigkeit
        - Vertraulichkeit
        - Integrität
        - Verfügbarkeit
        - Belastbarkeit
- Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

8. Unterstützungspflichten des Auftragsverarbeiters

- Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO, bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.
- Der Auftragsverarbeiter wird den Auftraggeber ferner gemäß Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung

der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

9. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

- Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind unter https://www.calenso.com/subprocessors aufgelistet. Für die aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, oder bestehende Subunternehmer durch neue zu ersetzen, wird er dies dem Auftraggeber in schriftlicher Form (z.B. per E-Mail oder Release-Notes auf dem Calenso Dashboard) anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt kein Einspruch durch den Auftraggeber innerhalb von 28 Tagen, dürfen die betroffenen Subunternehmer eingesetzt werden oder der Auftraggeber erhält ein außerordentliches Kündigungsrecht.
- Mit der Signatur dieses Vertrages stimmt der Auftraggeber den durch den Auftragnehmer beauftragten Subunternehmen, welche in Anhang C aufgelistet sind, zu. Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Erteilt der Auftragsverarbeiter mit Zustimmung des Auftraggebers Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten sowie die erforderliche Verpflichtung auf § 203 StGB aus diesem Vertrag dem Subunternehmer zu übertragen. Der Auftragsverarbeiter hat die Einhaltung der Pflichten der Subunternehmer zu überprüfen: Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

- Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.
- Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.
- Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.
- Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
- Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.
- Die Option zur Anbindung der Dienste von Anbietern außerhalb der EU bzw. des EWR steht dem Auftraggeber technisch zur Verfügung. Diese Anbindungen sind in der Grundkonfiguration nicht existent, sondern benötigen die aktive Einrichtung durch den Auftraggeber, um diese zu etablieren. Da es sich technisch nicht unterbinden lässt, weist der

Auftragsverarbeiter auf folgendes hin: Nimmt der Auftraggeber die Einrichtung einer solchen Anbindung vor, und handelt es sich um eine Einbeziehung von Subunternehmern in einem Drittland derart, dass die Daten Dritten außerhalb der EU oder des EWR zugänglich gemacht werden würden oder die Daten außerhalb der EU oder des EWR verarbeitet werden würden, ist dies unzulässig, da das für den Auftraggeber geltende Datenschutzrecht dadurch nicht eingehalten werden kann bzw. die Regeln zur berufsgruppenbezogenen Schweigepflicht aus § 203 StGB durch die Weitergabe verletzt werden würden.

10. Mitteilungspflichten des Auftragsverarbeiters

- Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.
- Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.
- Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.
- Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.
- Der Auftragsverarbeiter unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.
  Die Information enthält mindestens eine Beschreibung
  - der Art der Verletzung des Schutzes der Daten des Auftraggebers mit der Angabe der Kategorie(n) und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorie(n) und der ungefähren Zahl der betroffenen personenbezogener Datensätze

- der möglichen Folgen der Verletzung des Schutzes der Daten des Auftraggebers und ggf. Maßnahmen zur Abmilderung ihrer Auswirkungen.

11. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

12. Datengeheimnis und Vertraulichkeit

- Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt, zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.
- Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.
- Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

13. Schlussbestimmungen

- Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.
- Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.
- Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
- Sämtliche Anhänge zu diesem Vertrag sind Vertragsbestandteil.

_____	_____
Auftraggeber	**Marvin Felder** CEO Calenso AG

2. Anhang A

Einzelne Verarbeitungstätigkeiten

Werden personenbezogene Daten der betroffenen Person verarbeitet?

☒ Ja ☐ Nein

Zweck der Auftragsverarbeitung	Der Auftragsverarbeiter stellt eine Webanwendung zur Buchung von Terminvereinbarungen zwischen den Kunden des Auftraggebers und dem Auftraggeber bereit. Die erhobenen Kundendaten werden zum Zweck der eindeutigen Zuordnung der Person zu den von ihr gebuchten Terminen verwendet. Hierfür sind Vor- und Nachnamen essentiell und hinreichend. Die Erhebung von weiteren Daten sowie deren Zweck bestimmt der Auftraggeber.
Bezeichnung Verarbeitungstätigkeit	Online-Terminverwaltung
Subunternehmen	Die Beauftragung von Subunternehmern durch den Provider ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden Anhänge erfüllen. Eine Liste der aktuellen Subunternehmer ist dem Anhang C zu entnehmen, sowie unter https://www.calenso.com/subprocessors aufrufbar.
Art der personenbezogenen Daten (Datenarten bzw. -kategorien)	**Kunden des Auftraggebers** - Name - E-Mail-Adresse - weitere Kontaktinformationen - sämtliche Termininhalte und Termindaten Weitere Daten können vom Auftraggeber in der Anwendung als Felder hinzugefügt werden. Die Rechtmässigkeit der Felder obliegt nicht der Prüfung durch Calenso. Es dürfen keine besonderen personenbezogene Daten nach Artikel 9 DSGVO darüber verarbeitet werden. **Mitarbeiter des Auftraggebers** - Benutzername - Passwort (als Hash)

Aufbewahrungsdauer	- Für die Löschung und Archivierung der Kunden- und Kalenderdaten ist der Auftragsverarbeiter verantwortlich. Der Auftraggeber stellt diese Daten über die Laufzeit des Vertrages zur Verfügung. - Benutzerdaten (Mitarbeiter des Auftraggebers) und Login-Informationen werden über die gesamte Vertragslaufzeit gespeichert.
Löschfristen	- Löschung mit Vertragsbeendigung oder Kündigung mit erteiltem Löschauftrag. - Automatisierte, fristgebundene Löschung, wenn diese durch den Auftraggeber eingerichtet oder die Einrichtung dem Auftragsverarbeiter in Auftrag gegeben wurde. - Alle Daten (Profil, Kunden, Termine, Anmeldungen, etc.) können im Profil vor Vertragsbeendigung als Excel-Datei (xlsx) exportiert bzw. archiviert werden.
Garantien	Der Speicherort der Datenverarbeitung für die Anwendung liegt in der Schweiz.
Spezielle Sicherheitsmassnahmen (wenn nicht bereits im Allg. Sicherheitskonzept)	Calenso verfügt über ein Sicherheitskonzept. Aus Sicherheitsgründen wird dieses nicht öffentlich zugänglich gemacht. Nach dem Unterzeichnen einer Verschwiegenheitserklärung (NDA) wird das Sicherheitskonzept gerne an Kunden ausgehändigt. Um es anzufordern, schicken Sie bitte eine Nachricht an datenschutz@calenso.com.

3. Anhang B

Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

Unser Rechencenter-Betreiber «Nine Internet Solutions AG» ist ISO 27001 und ISO 9001 zertifiziert. Die nachfolgende Liste beinhaltet nur die technischen und organisatorischen Maßnahmen von Calenso, nicht die des Rechencenter-Betreibers.

4. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. DSGVO

Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
- Büroräume nur mit Schlüssel und Badge betretbar - Besucher haben keinen direkten Zugang zu den Büroräumen (digitale Schlösser)	- Besucher in Begleitung durch Mitarbeiter (nach Anmeldung)

Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
- Login mit Benutzername und Passwort - Anti-Viren Software Server - Anti-Viren Software Clients - Verschlüsselung von Mitarbeiter Notebooks / Tablets	- Verwalten von Benutzerberechtigungen - Erstellen von Benutzerprofilen - Richtlinie «Sicheres Passwort»(gemäss OWASP Vorgabe) - Allgemeine Richtlinie Datenschutz und / oder Sicherheit

Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
- Trennung von Produktiv- und Testumgebung - Physikalische Trennung (Systeme / Datenbanken / Datenträger) - Mandantenfähigkeit relevanter Anwendungen - Zugriff auf Server-Infrastruktur nur via VPN ins Calenso-Büro aus möglich (fixe IP) - Mitarbeiter Computer sind durch interne Firewall geschützt	- Verwalten von Benutzerrechte durch Administratoren - Einsatz Berechtigungskonzept - Minimale Anzahl an Administratoren - Steuerung über Berechtigungskonzept - Festlegung von Datenbankrechten - Datensätze sind mit Zweckattributen versehen

Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO, Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
Keine	- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

5. Integrität (Art. 32 Abs. 1 lit. B DSGVO)

Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
- Protokollierung der Zugriffe und Abrufe - Bereitstellung über verschlüsselte Verbindungen wie sftp, https - Zugriff auf Datenbank und Server nur via Calenso-VPN	Keine

Eingabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
- Audit-Logs, welche alle Erstellungen, Veränderungen und Löschungen von Kundendaten protokolliert - Zugriff auf Datenbank und Server nur via Calenso-VPN	- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können. - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen). - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. - Klare Zuständigkeiten für Löschungen.

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

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

Technische Maßnahmen	Organisatorische Maßnahmen
- Kunde kann selbst definieren, ob der Calenso-Support Zugriff auf die Kundendaten haben darf oder nicht	- Backup und Recovery-Konzept (alle 6 Stunden) - Kontrolle des Sicherungsvorgangs - Regelmäßige Tests zur Datenwiederherstellung - Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums - Jährlicher ausführlicher Penetrationtest durch OneConsult AG - Regelmäßiger VAPT (Vulnerability Assessment and Penetration-Test) von spezifischen Funktionen durch ViitorCloud Ltd.

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32. 1 lit. d DSGVO, Art. 25. Abs. 1 DSGVO)

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
- Anderweitig dokumentiertes Sicherheitskonzept - Eine Überprüfung der Wirksamkeit der technischen Schutzmassnahmen wird mindestens jährlich durchgeführt	- Interner und externer Datenschutzbeauftragter (Ralf Triebel, Calenso AG, datenschutz@calenso.com) - Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet - Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich) - Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
- Einsatz von Spamfilter und regelmässige Aktualisierung - Einsatz von Virenscanner und regelmäßige Aktualisierung	Keine

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.	Keine

Geprüft am **07.11.2024** durch **Ralf Triebel** (Datenschutzbeauftragter Calenso AG).

Ergebnisse:

☒ TOM sind für den angestrebten Schutzzweck ausreichend

☒ Vereinbarung Auftragsverarbeitung kann geschlossen werden

8. Anhang C

Liste der datenverarbeitenden Unternehmen, welche mit Calenso in Verbindung stehen.

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
Adobe Systems Software Ireland Ltd. 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin, D24 DCW0, Irland	Die Calenso Applikation (nur Buchungsprozesse) wird mit Adobe Launch überwacht, wenn vom Account-Inhaber das Adobe Launch Tracking aktiviert wurde.	Nein	Ja, wenn aktiviert	EU
Anthropic PBC 500 Howard Street, San Francisco, CA 94105, United States	Anbieter eines KI-Sprachmodells, das zur Verarbeitung und Generierung von Antworten im Support-Chat verwendet wird	Nein	Nein	USA
Apple Distribution International Ltd. Hollyhill Ln, Hollyhill Industrial Estate, Cork, T23 YK84, Irland	Kalender-Synchronisierung mit iCloud – Kalender wenn aktiviert	Nein	Ja, wenn aktiviert	EU
Atlassian Pty Ltd (Jira) Level 6, 341 George Street, Sydney NSW 2000, Australia	Tool zur Fehlerverfolgung und zum Projektmanagement für Entwicklung, Support und Unternehmenskundenprojekte	Nein	Nein	EU
bexio AG Alte Jonastrasse 24, 8640 Rapperswil, CH	Abwicklung der Rechnungen für jährliche Calenso Abonnemente. Endnutzer Daten werden für Rechnungsstellung verarbeitet und gemäß gesetzlicher Vorschriften gespeichert.	Nein	Ja, wenn aktiviert	CH
Cisco Systems GmbH Parkring 20, 85748 Garching, DE	Durchführung von Video-Meeting mit Meeting-Anbieter Webex	Nein	Ja, wenn aktiviert	EU
Cyon GmbH Brunngässlein 12, 4052 Basel, CH	Web-Hosting Anbieter mit Sitz in der Schweiz, welcher das Calenso Backup zweimal täglich abspeichert.	Ja	Ja, verschlüsselt	CH

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
dormakaba Deutschland GmbH **Access Solutions DACH** DORMA Platz 1, 58256 Ennepetal, DE	Digitale Schließ- und Zutrittslösung für Raumbuchungen	Nein	Nein	EU
Exoscale Boulevard de Grancy 19A, 1006 Lausanne, CH	Hosting des Meeting-Providers meet.calenso.com	Nein	Ja, wenn aktiviert	CH
F24 AG Samstagernstrasse 45, 8832 Wollerau, CH	SMS Anbieter mit Sitz in der Schweiz.	Nein	Ja, wenn aktiviert	CH
Freshworks Inc. 2950 S. Delaware Street, Suite 201, San Mateo CA 94403, USA	Support-Portal / Ticket-Portal. In Freshdesk werden alle Supportanfragen gespeichert und beantwortet.	Nein	Abhängig von Supportanfrage	EU
Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Die Calenso Applikation (nur Buchungsprozesse) wird mit Google Analytics überwacht, wenn der Google Tag Manager (GTM) vom Account-Inhaber aktiviert wurde. Kalender-Synchronisierung mit Google-Kalender, wenn aktiviert.	Nein	Ja, wenn der Google-Kalender angebunden wird	EU
GoTo Technologies Ireland Unlimited Company 10 Hanover Quay, Dublin, D02 R573, Irland	Durchführung von Video-Meeting mit Meeting-Anbieter GoToMeeting	Nein	Ja, wenn aktiviert	EU

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
Haufe-Lexware GmbH & Co. KG Munzinger Straße 9 79111 Freiburg, DE	Endnutzer Daten werden für Rechnungsstellung verarbeitet und gemäß gesetzlicher Vorschriften gespeichert.	Nein	Ja, wenn aktiviert	EU
Hostpoint AG Neue Jonastrasse 60, 8640 Rapperswil-Jona, CH	Web-Hosting Anbieter mit Sitz in der Schweiz, welcher das Calenso Backup zweimal täglich abspeichert.	Ja	Ja, verschlüsselt	CH
HubSpot, Inc. 25 First Street, Cambridge, MA 02141, United States	CRM-Plattform für das Kundenbeziehungsmanagement und den Versand von Marketingmitteilungen (Newsletter, Service- und Subprozessor-Benachrichtigungen)	Nein	Nein	EU
LINK Mobility Poland sp. z o. o. Toszecka 101, 44-100 Gliwice, PL	SMS-Anbieter mit Sitz in Europa.	Nein	Ja, wenn aktiviert	EU
Lovable Labs, Inc. 548 Market Street, San Francisco, CA 94104, United States	Plattform, die Tools wie das Calenso-Hilfezentrum bereitstellt	Ja	Nein	USA
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA	Kalender-Synchronisation, wenn aktiviert: Office 365, Exchange online Meeting Anbieter, wenn aktiviert: MS Teams	Nein	Ja, wenn aktiviert	EU
monday.com Ltd. 6 Yitzhak Sadeh Street, Tel Aviv 6777506, Israel	Projektmanagement- und Kollaborationsplattform für Unternehmenskunden	Nein	Abhängig von Unternehmenskunden-Anfrage	EU

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
Myra Security GmbH Landsberger Straße 181, 80687 München, DE	Zertifizierte Hyperscale WAF (Web Application Firewall) (ISO 27001, BSI C5, PCI-DSS, IDW PS 951/ISAE 3402, DSGVO). Die WAF filtert den Calenso Web Verkehr und schützt die Infrastruktur von Angriffen oder Bedrohungen (z.B. DDoS Attacken).	Ja	Ja, verschlüsselt	EU
New Relic 188 Spear St., Suite 1000, San Francisco, CA 94105, USA	Netzwerkanalyse Monitoring Bottleneck und Bug Detection	Ja	Nein	EU
Nine Internet Solutions AG Badenerstrasse 47, 8004 Zürich, CH	Haupt-Rechenzentrum für die Calenso-Applikation	Ja	Ja, verschlüsselt	CH
OpenAI, LLC 1455 3rd Street, San Francisco, CA 94158, United States	Anbieter von KI-Sprachmodellen zur Unterstützung automatisierter und assistierter Antworten im Support-Chat	Nein	Nein	USA
PayPal Pte. Ltd. 5 Temasek Boulevard #09-01 Suntec Tower Five Singapore 038985	Abwickler für Kreditkarten-Zahlungen von Terminbuchungen.	Nein	Ja, wenn aktiviert	EU
Pinecone Systems, Inc. 303 2nd Street, Suite 300, San Francisco, CA 94107, United States	Vektordatenbank zum Speichern und Abrufen von Wissen für den Support-Chat (semantische Suche und Abruf)	Nein	Nein	USA
salesforce.com Germany GmbH Erika-Mann-Str. 31, 80636 München, DE	Synchronisierung von Kunden- und Termindaten mittels Salesforce AppExchange App.	Nein	Ja, wenn aktiviert	EU

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
Sendinblue GmbH Köpenicker Str. 126, 10179 Berlin, DE	E-Mail und SMS-Anbieter mit Sitz in der EU.	Ja, opt-out möglich	Ja	EU
SIX Payment **Worldline Schweiz AG** Hardturmstrasse 201, CH-8005 Zürich, CH	Abwickler für Kreditkarten-Zahlungen von Terminbuchungen.	Nein	Ja, wenn aktiviert	CH
Skribble AG Förrlibuckstrasse 190, 8005 Zürich, CH	eSignature- Anbieter: Abwicklung der AV- Vertragsabschlüsse gemäss DSGVO, sowie der Reseller-Verträge.	Nein	Nein	CH
Stripe 510 Townsend St, San Francisco, CA 94103, USA	Abwickler für Kreditkarten-Zahlungen von Terminbuchungen.	Nein	Ja, wenn aktiviert	USA
Supabase, Inc. 3500 S. DuPont Highway, Dover, DE 19901, United States	Backend-Datenbankinfrastruktur für den Support-Chat	Nein	Nein	USA
Unblu Inc. Centralbahnplatz 10, 4051 Basel, CH	Durchführung von Video-Meeting mit Meeting-Anbieter Unblu Co-Browsing.	Nein	Ja, wenn aktiviert	CH
Zendesk, Inc. 989 Market Street, San Francisco, CA 94103, United States	Kundensupport und Ticketing-System zur Verwaltung von Supportanfragen und Kommunikation	Nein	Abhängig von Supportanfrage	EU

Unternehmen	Funktion / Beschreibung	Als Standard aktiv?	Übermittlung von Endkundendaten?	Daten-standort
Zoom Video Communications, Inc. 6601 College Blvd, Overland Park, KS 66210, USA	Durchführung von Video-Meeting mit Meeting-Anbieter ZOOM	Nein	Ja, wenn aktiviert	EU