Ergänzende vertragliche Bedingungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO für Kunden der Seconos

§ 1 Anwendungsbereich, Gegenstand und Dauer des Auftrags

(1) Anwendungsbereich

Die „Ergänzende vertragliche Bedingungen zur Auftragsverarbeitung“ (nachstehend „Vereinbarung“) konkretisiert die Verpflichtungen der Parteien zu den Anforderungen des Datenschutzes im Rahmen des zwischen den Parteien geschlossenen Hauptvertrags in seiner Ausformung durch die Allgemeinen Geschäftsbedingungen und der weiteren vertraglichen Vereinbarungen. Diese ergänzende Vereinbarung steht unter der Bedingung, dass entsprechend des Hauptvertrags eine Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 DSGVO erfolgt. Die Vereinbarung gilt entsprechend für die Prüfung, Fernprüfung und Wartungsdienstleistungen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Der Auftraggeber kann dieser Vereinbarung widersprechen, wenn es im Hauptvertrag im konkreten Einzelfall um eine Produktnutzung geht, bei der keine personenbezogenen Daten im Auftrag verarbeitet werden. Mit dem Widerspruch sichert der Auftraggeber dem Auftragnehmer zu, dass keine Verarbeitung stattfindet, die eine Vereinbarung zur Auftragsverarbeitung erfordert

(2) Gegenstand

Der Gegenstand des Auftrags im Sinne der Vereinbarung ergibt sich aus dem Hauptvertrag in seiner Ausformung durch die Allgemeinen Geschäftsbedingungen. Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Hauptvertrag. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Gegenstand der Verarbeitung personenbezogener Daten sind die Datenarten/-kategorien, welche dem Auftragnehmer im Rahmen seiner Dienstleistung bekannt werden können. Betroffen von der Verarbeitung sind insbesondere, aber nicht zwingend Kunden, Beschäftigte, Lieferanten, Handelsvertreter und Ansprechpartner. Die konkreten Umstände ergeben sich aus dem Hauptvertrag.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(3) Dauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Sofern keine Laufzeit im Hauptvertrag bestimmt wurde oder der Hauptvertrag in einer einmaligen Ausführung besteht, gilt der Vertrag als unbefristet und kann von beiden Parteien mit einer Frist von 4 Wochen zum Monatsende gekündigt werden. Die Möglichkeiten zur fristlosen Kündigung bleiben hiervon unberührt.

§ 2 Technisch Organisatorische Maßnahmen

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Der Auftraggeber und der Auftragsverarbeiter sind sich einig, dass die in der Anlage definierten TOMs ausreichend im Sinne der DSGVO sind. Die Einzelheiten der TOMs können Sie unter https://static.seconos.com/doc/TOM.pdf einsehen. Die Dokumentation der TOMs beinhaltet auf Aufforderung des Auftraggebers

auch Nachweise über das nach Art. 32 Abs. 1 lit. d) einzurichtende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

§ 3 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

Für geringfügige Ersuchen fallen keine Mehrkosten an. Darüber hinausgehende Aufwendungen hat der Auftraggeber mit einem angemessenen Entgelt entsprechend der konkreten Aufwendungen des Auftragnehmers zu vergüten.

§ 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten finden Sie in der Datenschutzerklärung unter https://seconos.com/datenschutz.html
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten **in Anlage 1**).
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Der Auftragnehmer unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten.

§ 5 Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Eine Liste der aktuell vom Auftragnehmer in Anspruch genommenen weiteren Auftragsverarbeitern finden Sie unter https://static.seconos.com/doc/UV.pdf. Der

Auftraggeber ermächtigt den Auftragnehmer mit der Unterzeichnung der Anlage, die dort aufgeführten Unternehmen in Anspruch zu nehmen. Die Hinzuziehung oder Ersetzung eines weiteren Auftragsdatenverarbeiters gilt als genehmigt, wenn der Auftragnehmer den Auftraggeber hierüber informiert hat und wenn der Auftraggeber innerhalb von 3 Monaten nach dieser Information keine Einwände gegenüber in schriftlicher oder elektronischer Form erhebt.

Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

Zieht der Auftragnehmer einen weiteren Auftragsverarbeiter in einem Drittland (außerhalb der EU/EWR) hinzu, wird der Auftragsverarbeiter insbesondere die Vorgaben gemäß Art. 44 ff. DSGVO beachten. Der Auftragnehmer wird hinreichende Garantien dafür vorsehen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen und Übermittlungen in ein Drittland und Schutzvorkehrungen gemäß Art. 30 Abs. 2 DSGVO dokumentiert werden.

§ 6 Kontrollbefugnisse

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

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. § 38 BDSG bzw. ab dem 25.05.2018 nach Art. 58 DSGVO i.V.m. § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

§ 7 Rechte und Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren, sowie Nachweise über die Einhaltung der in diesem Vertrag niedergelegten Pflichten anzufordern. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

Gegen die Auswahl von Dritten hat der Auftragnehmer ein Widerspruchsrecht, insofern es sich um einen Mitbewerber des Auftragnehmers handelt. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie in diesem Vertrage vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

§ 8 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen.

§ 9 Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis nach Wahl des Auftraggebers entweder

zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Löschung oder Sperrung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe, Löschung oder Sperrung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden und hat in analoger Anwendung der Grenzen des § 8 zu erfolgen.

§ 10 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

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