

Auftragsverarbeitung gemäß Art. 28 DS-GVO

1. Gegenstand und Dauer des Auftrags

- 1.1 Der Auftragsverarbeiter estos GmbH (im Folgenden „Auftragnehmer“) verarbeitet personenbezogene Daten im Auftrag des Auftraggebers (Auftragsverarbeitung). Dies umfasst alle Tätigkeiten, die der Auftragnehmer im Rahmen der Erfüllung des Vertrags (im Folgenden „Hauptvertrag“) mit dem Auftraggeber erbringt und die eine Auftragsverarbeitung darstellen.
- 1.2 Der Gegenstand des Auftrags ergibt sich aus den Regelungen des Hauptvertrags.
- 1.3 Die im Hauptvertrag getroffenen Regelungen zu Laufzeit und Kündigung finden analog Anwendung.

2. Konkretisierung des Auftragsinhalts

- 2.1 Der Auftraggeber oder der Verantwortliche betreiben estos Software Produkte unter eigener Hoheit, die den in der Produktdokumentation beschriebenen Funktionsumfang bereitstellen. Der Auftragnehmer leistet generelle technische Unterstützung oder nimmt seine gesetzlichen oder vertraglichen Verpflichtungen zur Beseitigung von Mängeln wahr. Aus organisatorischen Gründen wird zur Verwaltung der Kundenvorgänge Software (Ticketsystem) eingesetzt. Zur Bearbeitung der Kundenvorgänge werden personenbezogene Daten vom Auftraggeber im Ticketsystem hinterlegt, dort gespeichert und elektronisch verarbeitet.
- 2.2 Gegenstand der Verarbeitung personenbezogener Daten sind, (a) Name, Kundennummer, (b) Adresse, Abteilung, (c) Kommunikationsdaten (E-Mail, Telefonnummer, Fax usw.) und (d) Journale und Verbindungsprotokolle
- 2.3 Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen, (a) Beschäftigte des Auftraggebers, (b) Kunden des Auftraggebers sowie deren Beschäftigte, (c) Interessenten und Geschäftskontakte des Auftraggebers, (d) Lieferanten, (e) Handelsvertreter und (f) Sonstige Ansprechpartner.

3. Pflichten des Auftragnehmers

- 3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

- 3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt (Die technisch-organisatorischen Maßnahmen des Auftragnehmers können in ihrer jeweils aktuellen Fassung auf der Webseite des Auftragnehmers eingesehen werden ([Link](#))). Der Auftraggeber hat die im Vorfeld der Auftragsvergabe dort dokumentierten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Auftragsverarbeitung geprüft. Sie sind Grundlage dieses Auftrags. Soweit spätere Prüfungen/Audits einen Anpassungsbedarf ergeben, ist dem einvernehmlich Rechnung zu tragen. Eine Änderung der getroffenen Sicherheitsmaßnahmen in Anbetracht des technischen Fortschritts und der Weiterentwicklung bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
- 3.3 Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten.
- 3.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht wurden und sich zur Vertraulichkeit verpflichtet haben sowie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- 3.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten, die er für den Auftraggeber verarbeitet, bekannt werden.

- 3.6 Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- 3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- 3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- 3.9 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
- 3.10 In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
- 3.11 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
- 3.12 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer wirtschaftlich vertretbare Anstrengungen zu unternehmen um den Auftraggeber bei der Abwehr des Anspruches zu unterstützen.

4. Pflichten des Auftraggebers

- 4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- 4.2 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Ziffer 3. Abs. 10 entsprechend.

- 4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- 4.4 Für die Beurteilung der Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Artt. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich (siehe auch nachfolgend Ziffer 5).
- 4.5 Der Auftraggeber erteilt alle Aufträge, Teilaufträge, Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.
- 4.6 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5. Anfragen betroffener Personen

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung von dessen Pflicht, Anträge von Betroffenen zu bearbeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

- 6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Dazu gewährleistet der Auftragnehmer unter anderem die Einhaltung folgender Vorgaben.

(a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(b) Die Wahrung der Vertraulichkeit gemäß Artt. 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.

(c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO. Diese sind in ihrer jeweils aktuellsten Fassung auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf die im Auftrag verarbeiteten Daten erstreckt. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten beim Auftragnehmer ermittelt.

(f) 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, wird ihn der Auftragnehmer im Rahmen seiner Möglichkeiten mit wirtschaftlich vertretbarem Aufwand unterstützen.

(g) 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 ein angemessener Schutz der Rechte der betroffenen natürlichen Person gewährleistet wird.

- 6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Unter keinen Umständen dürfen die Bedingungen dieser Inspektion jedoch den Schutz der Daten

der anderen Kunden des Auftragnehmers beeinträchtigen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

- 6.3 Für die Unterstützung bei der Durchführung einer Inspektion einigen sich Auftragnehmer und Auftraggeber im Vorfeld auf eine angemessene Vergütung. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten aktuellen Testats, von Berichten und Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzaudatoren oder Qualitätsaudatoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der nach diesem Vertrag geschuldeten technischen und organisatorischen Maßnahmen zu überzeugen.
- 6.4 Das Recht der Datenschutzaufsichtsbehörde oder einer sonstigen hoheitlichen Aufsichtsbehörde gem. Art. 28 Abs. 3 lit. h DS-GVO eine Inspektion der Räumlichkeiten vorzunehmen, bleibt unberührt. Im Übrigen gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7. Subunternehmer (weitere Auftragsverarbeiter)

- 7.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung (a) andere verbundene Unternehmen des Auftragnehmers als Unterauftragnehmer hinzuzuziehen, und (b) erteilt dem Auftragnehmer und seinen verbundenen Unternehmen die Ermächtigung, Dritte als Unterauftragsnehmer zu beauftragen.
- 7.2 Der Auftragnehmer führt auf seiner Homepage eine Liste mit den aktuell beauftragten Unterauftragnehmern ([Link](#)). Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.
- 7.3 Der Auftraggeber kann der Änderung – innerhalb einer Frist von zehn (10) Tagen – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle schriftlich widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, werden die Parteien innerhalb eines Zeitraums von vierzehn (14) Tagen

versuchen eine einvernehmliche Lösung zu finden. Nach erfolglosem Ablauf der Frist für das Einwandverfahren wird beiden Parteien ein Sonderkündigungsrecht für diesen Vertrag eingeräumt.

- 7.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer im Rahmen eines Auftragsverarbeitungsvertrages zu übertragen.
- 7.5 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

8. Informationspflichten

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.