

Hinweis

Das nachfolgende Vertragsmuster soll als Orientierungshilfe für Auftragsverarbeitungen dienen. Es muss auf jeden Fall für die konkrete Anwendung überprüft und wenn erforderlich an die individuellen Gegebenheiten angepasst werden. Die SYNAXON AG übernimmt keine Haftung für Schäden, die durch die Verwendung des Vertragsmusters entstehen.

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

.....

.....

.....

- Verantwortlicher, im Folgenden Auftraggeber genannt -

und der

.....

.....

.....

- Auftragsverarbeiter, im Folgenden Auftragnehmer genannt -

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Vertragsverhältnis über Wartung/Pflege/Betrieb von IT-Systemen (Managed Services) ergeben.

Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit der zugrundeliegenden Leistungsbeschreibung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten (Daten) des Auftraggebers in Berührung kommen können.

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags und damit der Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Technischer Support (z. B. Fernwartung), Wartungs-/Pflegearbeiten an IT-Systemen des Auftraggebers

Die Verarbeitung und Nutzung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff.

DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, verbindliche interne Datenschutzvorschriften, Standarddatenschutzklauseln, genehmigte Verhaltensregeln, genehmigter Zertifizierungsmechanismus).

1.2 Dauer

Die Dauer dieser Vereinbarung (Laufzeit) richtet sich nach der Laufzeit der Leistungsbuchung im Rahmen des jeweiligen Produktvertrages.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Datenverarbeitung

Zweck der Datenerhebung, -verarbeitung oder -nutzung ist technischer Support (z. B. über Fernwartung) sowie Wartungs-/Pflegearbeiten an IT-Systemen des Auftraggebers. Betroffen hiervon sind personenbezogene Daten und Systemdaten/technische Daten

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind Daten aus folgenden Datenkategorien:

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(Zutreffendes bitte ankreuzen/ergänzen)

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐ ...

(Zutreffendes bitte ankreuzen/ergänzen)

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, Anfragen von Betroffenen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

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

3.3 Der Auftraggeber ist berechtigt, sich wie unter Ziffer 8 festgelegt, vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

3.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.5 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

3.6 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.

4 Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers.

Sofern der Auftragnehmer zu einer anderen Verarbeitung gesetzlich verpflichtet ist (z. B. bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden), teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine vom Auftraggeber erteilte Weisung gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Umsetzung der entsprechenden Weisung solange auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wurde.

4.3 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.4 Kopien oder Duplikate der personenbezogenen Daten wird der Auftragnehmer ohne Wissen des Auftraggebers nicht erstellen. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

4.5 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

4.6 Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

4.7 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers wird der Auftragnehmer im notwendigen Umfang mitwirken und den Auftraggeber soweit möglich angemessen unterstützen.

4.8 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

4.9 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet.

4.10 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

4.11 Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung 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.

4.12 Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(Bitte ausfüllen oder löschen)

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

5.1 Dem Auftragnehmer ist bekannt, dass im Falle von Verletzungen des Schutzes personenbezogener Daten für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden der Verletzung vorsieht.

5.2 Der Auftragnehmer wird dem Auftraggeber daher unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie einen Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mitteilen.

5.3 Der Auftragnehmer trifft angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

5.4 Der Auftragnehmer wird den Auftraggeber erforderlichenfalls bei entsprechenden Meldepflichten angemessen unterstützen. Dies gilt sowohl für die Meldung einer etwaigen Pflichtverletzung gegenüber der Aufsichtsbehörde, als auch für die Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung vornehmen.

6 Unterauftragsverhältnisse mit Subunternehmern

6.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit schriftlicher Zustimmung des Auftraggebers gestattet.

Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.

Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

6.2 Eine Beauftragung von Subunternehmern, die die vereinbarten Leistungen außerhalb der EU / des EWR erbringen, darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

6.3 Der Auftragnehmer hat vertraglich sicherzustellen, dass die zwischen Auftraggeber und Auftragnehmer vereinbarten Regelungen auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.4 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.

6.5 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.6 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

6.7 Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

6.8 Vor der Hinzuziehung weiterer oder der Ersetzung bisheriger Subunternehmer wird der Auftragnehmer den Auftraggeber rechtzeitig schriftlich informieren. Der Auftraggeber kann der Änderung innerhalb einer Frist von zehn Werktagen aus wichtigem Grund widersprechen. Erfolgt kein schriftlicher Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als erteilt. Liegt ein wichtiger datenschutzrechtlicher Grund für einen Widerspruch des Auftraggebers vor und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, erhält der Auftraggeber ein Sonderkündigungsrecht.

6.9 Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7 Technisch-organisatorische Maßnahmen

7.1 Der Auftragnehmer gewährleistet für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau.

7.2 Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen. 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 DSGVO zu berücksichtigen

7.3 Die in Anlage 1 dokumentierten Maßnahmen stellen die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko dar.

7.4 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen.

7.5 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

7.6 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

7.7 Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

8 Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist - grundsätzlich nach Terminvereinbarung - berechtigt, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen beim Auftragnehmer im angemessenen und erforderlichen Umfang selbst oder durch im Einzelfall zu benennende Personen zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.

8.2 Der Auftraggeber wird Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

8.3 Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Er wird dem Auftraggeber auf Anforderung die erforderlichen Auskünfte erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachweisen.

8.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9 Berichtigung, Einschränkung und Löschung von Daten

9.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

9.2 Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen selbst darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

10.1 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber spätestens aber mit Beendigung des Hauptvertrages, hat der Auftragnehmer sämtliche in seinen Besitz sowie an Unterauftragnehmer gelangten Daten, Unterlagen, erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu löschen bzw. zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

10.2 Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Anforderung mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

11 Haftung

Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, es ist ausdrücklich etwas Anderes vereinbart.

12 Schlussbestimmungen

12.1 Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.2 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Hauptvertrages vor.

12.3 Es gilt deutsches Recht unter Ausschluss des materiellen internationalen Privat- sowie Kollisionsrechts.

12.4 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

Die folgenden Anlagen gelten als vertragswesentliche Bestandteile:

Anlage 1 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Anlage 2 Genehmigte Subunternehmer

.....
Ort, Datum

.....
Ort, Datum

.....
Auftragnehmer

.....
Auftraggeber

Anlage 1

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

(Bitte entsprechend ausfüllen)

Verantwortliche Stelle:

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

2. Integrität (Art. 32 Abs. 1b DSGVO)

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

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

Anlage 2

Genehmigte Subunternehmer

Name und Anschrift des Subunternehmers	Auftragsinhalt
SYNAXON AG Falkenstr. 31, 33758 Schloß Holte-Stukenbrock, DE	Support SYNAXON Managed Services

(bitte ggf. weitere Subunternehmer ergänzen)