Bedingungen zur Vereinbarung einer Auftragsverarbeitung von personenbezogenen Daten nach Art. 28 DSGVO

Definitionen und Anwendungsbereich

Mit „**Auftraggeber**“ ist nachfolgend jedes Unternehmen gemeint, welches mit der itsm IT-Systeme & Management GmbH, Hauptstraße 82, 08427 Fraureuth unter Einbeziehung der Allgemeinen Geschäftsbedingungen der itsm IT-Systeme & Management GmbH sowie unter Einbeziehung der Besonderen Vertragsbedingungen Besonderen Vertragsbedingungen für den Kauf von pds Standardsoftwareprodukten (**„BV-Kauf**“), für SaaS-Leistungen (**„BV-SaaS**“), für Softwarepflege (**„BV-Pflege**“), für pds App-Dienste (**„BV-App**“), für die Nutzung der API **(„BV-API“),** für die Nutzung BI **(„BV-BI**“) und/oder für die Erbringung von Rechenzentrumsleistungen „pds Cloud“ (**„BV-RZ**“) einen oder mehrere Überlassungsverträge, SaaS-Verträge, Pflegeverträge, Nutzungsverträge und/oder RZ-Verträge abgeschlossen hat.

Mit „**Auftragnehmer**“ ist nachfolgend die itsm IT-Systeme & Management GmbH, Hauptstraße 82, 08427 Fraureuth gemeint.

Mit „**Hauptvertrag**“ ist nachfolgend der jeweilige zwischen Auftraggeber und Auftragnehmer abgeschlossene Überlassungsvertrag, SaaS-Vertrag, Pflegevertrag, Nutzungsvertrag und/oder RZ-Vertag gemeint.

Mit „**Vertrag**“ oder „**Vereinbarung**“ sind nachfolgend diese Bedingungen zur Vereinbarung einer Auftragsverarbeitung von personenbezogenen Daten nach Art. 28 DS-GVO, einschließlich der „**Anlage 1 – Unterauftragsverarbeiter**“ und der „**Anlage 2 – Technische und organisatorische Maßnahmen**“ gemeint.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den im Hauptvertrag vereinbarten Leistungen ergeben. Der Anwendungsbereich erstreckt sich auf alle Tätigkeiten, die mit dem Hauptvertrag in Verbindung stehen und die eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Rahmen einer Auftragsverarbeitung im Sinne des Art. 28 DS-GVO für den Auftraggeber zum Gegenstand haben.

§ 1 Gegenstand und Dauer des Vertrags

(1) Der Gegenstand und die Dauer des Vertrags ergeben sich aus dem Hauptvertrag.
(2) Der Auftragnehmer führt zur Vertragserfüllung Tätigkeiten aus, im Rahmen derer die Verarbeitung von Daten mit Personenbezug für den Auftraggeber möglich ist.
(3) Die Regelungen dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen Gegenstand der Tätigkeiten des Auftragnehmers ist und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 2 Art, Umfang und Zweck der Datenverarbeitung

(1) Art, Umfang und Zweck der Datenverarbeitung ergeben sich aus dem Hauptvertrag.

§ 2.1 Kategorien der personenbezogenen Daten

(1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/Kategorien

a. Daten aus den betreuten Anwendungen der pds (Personen- und Vertragsstammdaten, Kommunikationsdaten, Abrechnungsdaten, archivierte Belege)
b. System-, Zugangs-, Steuerungs- und Sicherheitseinstellungen der betreuten Systeme
c. Konfigurations-, Steuerungs- und Hilfsdaten von Programmen, die zur Erfüllung der vertraglich geschuldeten Tätigkeiten vom Auftragnehmer benötigt werden, bspw. Updates, Virensignaturen

§ 2.2 Kategorien betroffener Personen

(1) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

a. Mitarbeiter des Auftraggebers
b. Lieferanten
c. Kunden
d. Interessenten

§ 3 Technische und organisatorische Maßnahmen

(1) 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. Die jeweils aktuellen TOM sind über den folgenden Link abrufbar und werden regelmäßig aktualisiert: https://www.itsm-gmbh.de/datenschutzerklaerung/
Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 Unterabs. 1 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. Einzelheiten sind in der Anlage 2 dokumentiert.

(3) 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.

§ 4 Berichtigung, Löschung und Sperrung von Daten

(1) 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.

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

(3) Die Weisung durch den Auftraggeber muss im Falle einer Löschung von Daten schriftlich erfolgen.

§ 5 Qualitätssicherung und Pflichten des Auftragnehmers

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

a. Bei dem Auftragnehmer ist als interner Beauftragter für den Datenschutz

ad hoc datenschutz GmbH
Im Bresselsholze 12
07819 Triptis

E-Mail: datenschutz@itsm-gmbh.de

bestellt. Über einen etwaigen Wechsel des Datenschutzbeauftragten wird der Auftraggeber informiert.

b. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 Unterabs. 1 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 siehe Anlage gemäß Art. 28 Abs. 3 Unterabs. 1 lit. c, 32 DS-GVO.
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 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.
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, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g. Der Auftragnehmer etabliert ein Verfahren zur regelmäßigen Kontrolle der internen datenschutzrelevanten Prozesse sowie der technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich sicher ist.
h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieses Vertrages.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 24 DS-GVO. Er ist für die Sicherstellung der Zulässigkeit der Datenverarbeitung und für die Wahrung der Rechte Betroffener verantwortlich.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten in der vom Auftragnehmer durchgeführten Datenverarbeitung feststellt.
(3) Die Pflicht zur Führung eines Verfahrensverzeichnisses gemäß Art. 30 EU-DSGVO liegt für ihren jeweiligen Zuständigkeitsbereich beim Auftraggeber und Auftragnehmer.
(4) Die Informationspflichten gegenüber den Betroffenen gemäß Art. 13 und 14 EU-DSGVO obliegen dem Auftraggeber.
(5) Wenn auf ausdrückliche Weisung des Auftraggebers Daten vom Auftragnehmer an den Auftraggeber übergeben werden sollen, trägt der Auftraggeber die dadurch entstehenden Kosten.
(6) Wenn durch vom Auftraggeber erteilte Weisungen Leistungen zu erbringen sind, die nicht durch diesen Vertrag (bzw. dem zugrundeliegenden Hauptvertrag) abgedeckt sind, wird der Auftragnehmer den Auftraggeber darüber zeitnah und unter Bezifferung des entstehenden Aufwands informieren. Die Kosten für die Umsetzung der Weisungen trägt der Auftraggeber.

§ 7 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu, die unter Einhaltung der Voraussetzungen gemäß Art. 28 Abs. 2–4 DSGVO beauftragt sind. Die jeweils aktuelle Liste der eingesetzten Unterauftragnehmer ist unter folgendem Link abrufbar: https://www.itsm-gmbh.de/datenschutzerklaerung/
(3) Dem Wechsel der bestehenden Unterauftragnehmer sowie die Hinzunahme neuer Unterauftragnehmer stimmt der Auftraggeber zu.
(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 dieser Vorschrift eingesetzt werden sollen.
(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von

der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a. Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
b. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

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

§ 9 Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und in zumutbarer Weise bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

b. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang relevante Informationen zur Verfügung zu stellen

c. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

d. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht im Hauptvertrag (Lizenzauftrag) enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird Daten des Auftraggebers nur zur Erfüllung der vertraglich vereinbarten Leistungen und nach Weisung des Auftraggebers erheben bzw. verarbeiten, nutzen oder speichern.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung des Auftraggebers gegen geltende datenschutzrechtliche Vorschriften oder die vertraglichen Vereinbarungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung

der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Weisungen erfolgen durch den Auftraggeber in Schriftform oder Textform (bspw. per E-Mail).

§ 11 Rückgabe überlassener Datenträger und Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 12 Durchführung der Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung bzw. per Fernzugriff auf den Systemen des Auftraggebers durchgeführt, gelten zusätzlich folgende Vereinbarungen:

(1) Der Auftragnehmer muss personenbezogene Daten, die er bei der Fernwartung erhalten oder gewonnen hat, unverzüglich sicher löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

(2) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen, Ausnahmen sind mit dem Auftraggeber abzustimmen.

(3) Die Mitarbeiter des Auftragnehmers verwenden nach dem Stand der Technik hinreichend sichere Identifizierungs- und Einwahlverfahren. Die Fernwartung darf nur über nach dem Stand der Technik sichere Leitungen abgewickelt werden.

(4) Wird die Fernwartung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Serviceleistung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung von der Wartungszentrale aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

§ 13 Home-Office

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) unter Einhaltung der Regelungen der nachfolgenden Absätze erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten

technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform (z.B. E-Mail) zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach den Absätzen 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle im „Home-Office“ von Beschäftigten durch den Auftragnehmer zu ermöglichen.

§ 14 Sonstige Informationspflichten, Schriftformklausel, Rechtswahl

(1) 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 Stelle“ im Sinne der Datenschutzgesetze liegen.

(2) Änderungen und Ergänzungen dieses Vertrags und aller Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung 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.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

…….. ……..

Auftraggeber (Kunde)
Ort, Datum, Unterschrift

Auftragnehmer (itsm)
Ort, Datum, Unterschrift

Anlagen

Anlage 1 Unterauftragsverarbeiter

Anlage 2 Technische und organisatorische Maßnahmen