**Auftragsverarbeitungsvertrag**

**gemäß Art. 28 EU-Datenschutz-Grundverordnung (DSGVO)**

zwischen

**Name und Anschrift Auftraggeber (MAN)**

(nachfolgend „**Auftraggeber“** genannt)

und

**Name und Anschrift Auftragnehmer (Lieferant/Dienstleister)**

(nachfolgend „**Auftragnehmer“** genannt)

**§ 1 Gegenstand**

1. **Hauptvertrag.** Dieser Auftragsverarbeitungsvertrag regelt die Verpflichtungen der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer (**„Daten“**) im Rahmen des in Anlage 1 genannten Vertrages („**Hauptvertrag**“)

2. **Umfang.** Gegenstand, Umfang und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer ergeben sich aus Anlage 1 und der Leistungsbeschreibung des Hauptvertrages.

3. **Vorrangregelung**. Die Bestimmungen dieses Auftragsverarbeitungsvertrages einschließlich seiner Anlagen haben Vorrang gegenüber Bestimmungen des Hauptvertrages. Sollten die EU-Standardvertragsklauseln Vertragsbestandteil werden, haben sie Vorrang gegenüber den Bestimmungen dieses Auftragsverarbeitungsvertrages und seinen Anlagen.

**§ 2 Rechte und Pflichten des Auftraggebers**

1. **Rolle des Auftraggebers.** Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO oder (Unter-) Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO eines/mehrerer Verantwortlichen/Verantwortlicher bzw. eines/mehrerer anderen/anderer Auftragsverarbeiters/Auftragsverarbeiter, dessen/deren Daten er im (Unter-) Auftrag verarbeitet. Er ist insbesondere für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte der betroffenen Personen verantwortlich.

2. **Weisungen.** Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Der Auftraggeber erteilt Weisungen grundsätzlich schriftlich oder per E-Mail. Bei Eilbedürftigkeit oder aufgrund anderer besonderer Umstände können Weisungen auch mündlich oder fernmündlich erteilt werden, wobei diese unverzüglich vom Auftraggeber schriftlich oder per E-Mail zu bestätigen sind.

Die weisungsberechtigten Personen des Auftraggebers sowie die zuständigen Weisungsempfänger beim Auftragnehmer sind in Anlage 1 genannt. Änderungen der weisungsberechtigten Personen bzw. der zuständigen Weisungsempfänger sind der anderen Partei unverzüglich in Schriftform oder per E-Mail anzuzeigen.

**§ 3 Rechte und Pflichten des Auftragnehmers**

1. **Rolle des Auftragnehmers.** Der Auftragnehmer ist (Unter-) Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

Der Auftragnehmer einschließlich der von ihm eingesetzten Personen, die Zugang zu den Daten haben, verarbeiten die Daten ausschließlich für die in Anlage 1 genannten Zwecke und im Rahmen des Hauptvertrages gemäß den Weisungen des Auftraggebers - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation -,
sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedstaaten zu einer bestimmten Verarbeitung verpflichtet ist; der Auftragnehmer teilt dem Auftraggeber vor der Verarbeitung eine solche gesetzliche Verpflichtung mit, sofern dies nicht wegen eines wichtigen öffentlichen Interesses durch das betreffende Recht untersagt ist (Art. 28 Abs. 3 S. 2 a DSGVO).

Der Auftragnehmer dokumentiert die ihm erteilten Weisungen in geeigneter, übersichtlicher Form und stellt dem Auftraggeber diese Dokumentation auf Verlangen zur Verfügung.

Etwaige spezielle Weisungen zu Vertragsbeginn sind in Anlage 1 festgelegt. Kopien oder Duplikate der personenbezogenen 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 benötigt werden.

2. **Löschung, Rückgabe.** Nach Aufforderung durch den Auftraggeber oder unverzüglich nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer dem Auftraggeber sämtliche personenbezogenen Daten aus dem Auftragsverhältnis nach dessen Wahl auszuhändigen oder datenschutzgerecht zu vernichten bzw. zu löschen (dies gilt auch für eventuell vorhandene Kopien), sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragnehmer teilt dem Auftraggeber eine solche gesetzliche Verpflichtung mit, sofern dies nicht gesetzlich untersagt ist. Die Pflicht zur Löschung bzw. Aushändigung gilt auch für Test- und Ausschussmaterial. Die Löschung, Vernichtung oder vollständige Aushändigung ist dem Auftraggeber mit Datumsangabe in schriftlicher Form zu bestätigen. Die Einrede von Zurückbehaltungsrechten, z.B. im Sinne von § 273 BGB, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

3. **Datenschutzbeauftragter bzw. Ansprechpartner Datenschutz.** Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten sind in Anlage 1 genannt. Änderungen sind dem Auftraggeber unverzüglich schriftlich oder per E-Mail mitzuteilen.

Soweit die Bestellung eines Datenschutzbeauftragten gesetzlich nicht vorgeschrieben ist, hat der Auftragnehmer einen Ansprechpartner Datenschutz ernannt oder wird diesen unverzüglich ernennen. Die Kontaktdaten des Ansprechpartners Datenschutz sind in Anlage 1 genannt. Änderungen sind dem Auftraggeber unverzüglich schriftlich oder per E-Mail mitzuteilen.

4. **Datengeheimnis.** Der Auftragnehmer ist verpflichtet, die Daten vertraulich zu behandeln. Der Auftragnehmer hat die Vorschriften der DSGVO zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 2 b, 29, 32 Abs. 4 DSGVO zu beachten. Der Auftragnehmer setzt demnach bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten anwendbaren Datenschutzgesetzen vertraut gemacht wurden. Die Vertraulichkeitsverpflichtung der Mitarbeiter des Auftragnehmers muss auch nach Beendigung ihres Arbeitsvertrages gelten. Diese Pflichten des Auftragnehmers gelten auch nach Beendigung dieses Auftragsverarbeitungsvertrages fort.

5. **Einhaltung gesetzlicher Vorschriften, Kontrolle.** Der Auftragnehmer ist verpflichtet, sämtliche ihn im Rahmen der Verarbeitung von Daten im Auftrag betreffenden anwendbaren gesetzlichen Vorschriften zu beachten. Er kontrolliert die Einhaltung der anwendbaren Datenschutzgesetze, seiner vertraglichen Verpflichtungen und der Weisungen des Auftraggebers regelmäßig während der Vertragslaufzeit und hat dies dem Auftraggeber auf Verlangen in geeigneter Form nachzuweisen. Die Kontrollpflicht gilt insbesondere für die internen Prozesse sowie die technischen und organisatorischen Maßnahmen. Die Maßnahmen zur Überwachung sind in einem Datenschutzkonzept zu beschreiben, das dem Auftraggeber auf Anforderung vorzulegen ist.

6. **Unterstützung des Auftraggebers bei Erfüllung von Pflichten nach der DSGVO.** Der Auftragnehmer wird angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen nachzukommen. Falls die betroffenen Personen ihre Rechte beim Auftragnehmer geltend machen, muss dieser die Anfragen unverzüglich an den Auftraggeber weiterleiten. Ausschließlich nach dokumentierter Weisung des Auftraggebers darf der Auftragnehmer den betroffenen Personen gegenüber Auskünfte erteilen, deren Daten berichtigen, löschen oder die Verarbeitung der Daten einschränken.

Der Auftragnehmer wird ferner unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen.

 Der Auftragnehmer wird den Auftraggeber im Übrigen bei der Beantwortung von behördlichen oder gerichtlichen Anfragen oder sonstigen behördlichen oder gerichtlichen Maßnahmen (z.B. Kontrollen) in angemessenem Umfang unterstützen und erforderliche Informationen zur Verfügung stellen.

7. **Datenschutzverletzungen**. Datenschutzverletzungen beim Auftragnehmer oder seinen Unterauftragnehmern sind dem Auftraggeber unverzüglich nach Bekanntwerden zu melden und es sind die Informationen und Unterlagen beizufügen, die zur Erfüllung eventueller Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 EU DSGVO erforderlich sind. Der Auftragnehmer hat hierbei alle wesentlichen Umstände, die ergriffenen Maßnahmen und eine Einschätzung der sich aus der Datenschutzverletzung erwachsenden Risiken für die betroffenen Personen mitzuteilen. Er wird Rückfragen unverzüglich beantworten und mit dem Auftraggeber bei der Aufklärung der Umstände eng kooperieren. Die Meldung einer Datenschutzverletzung an die zuständige Behörde und die Benachrichtigung der betroffenen Personen erfolgen ausschließlich durch den Auftraggeber.

Die Meldung des Auftragnehmers muss gleichzeitig an folgende E-Mail-Adressen erfolgen:

- E-Mail-Adresse des in Anlage 1 Ziffer 9 genannten Weisungsberechtigten

- Datenschutz-Funktionspostfach des Auftraggebers, Anlage 1 Ziffer 13.

**§ 4 Ort der Verarbeitung**

1. **Zustimmungserfordernis bei Verarbeitung im unsicheren Drittland.** Die Verarbeitung der Daten durch den Auftragnehmer und die vom Auftraggeber genehmigten Unterauftragnehmer
(s. § 7) findet grundsätzlich ausschließlich in der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem solchen Land statt, für das ein Angemessenheitsbeschluss der Europäischen Kommission gem. Art. 45 DSGVO vorliegt. Jede Verlagerung der Verarbeitung in ein sonstiges Land (**„unsicheres Drittland“**) bedarf der Zustimmung des Auftraggebers und darf zudem nur erfolgen, wenn die gesetzlichen Voraussetzungen für Datenübermittlungen in Drittländer nach den anwendbaren Datenschutzgesetzen erfüllt sind. Dazu sind Angaben in Anlage 1 und ggf. zusätzliche Unterlagen erforderlich.

2. **Verarbeitung durch Auftragnehmer im unsicheren Drittland.** Wenn die Verarbeitung der Daten durch den Auftragnehmer ausschließlich oder auch in einem unsicheren Drittland erfolgt, gelten die mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 erlassenen EU-Standardvertragsklauseln („**EU Standardvertragsklauseln 2021**“). Die Auswahl des auf die Verarbeitung anwendbaren Moduls dieser EU Standardvertragsklauseln ist in
Anlage 1 vorzunehmen.

 Bei der Dokumentation der Einhaltung der aus den EU Standardvertragsklauseln 2021 resultierenden Verpflichtungen werden Auftraggeber und Auftragnehmer eng zusammenarbeiten. Zur Erfüllung der in Klausel 14 der EU Standardvertragsklauseln 2021 genannten Kriterien ist der Auftragnehmer verpflichtet, dem Auftraggeber alle insoweit erforderlichen Informationen zur Verfügung zu stellen. Der Auftragnehmer wird dem Auftraggeber insbesondere Fragen wahrheitsgemäß, umfassend und innerhalb eines angemessenen Zeitraums beantworten, die die Anwendbarkeit von Rechtsvorschriften und Gepflogenheiten bzw. deren praktische Umsetzung in den relevanten unsicheren Drittländern betreffen.

Wenn aufgrund der Rechtsvorschriften und Gepflogenheiten in diesen unsicheren Drittländern und angesichts der besonderen Umstände der Verarbeitung keine hinreichende Gewähr dafür besteht, dass die Verarbeitung im Einklang mit den EU Standardvertragsklauseln 2021 erfolgt, wird der Auftragnehmer in Abstimmung mit dem Auftraggeber (i) zusätzliche technische und organisatorische Maßnahmen ergreifen und/oder (ii) zusätzliche vertragliche Zusicherungen abgeben, die unter Berücksichtigung dieser Rechtsvorschriften und Gepflogenheiten und der besonderen Umstände der Verarbeitung eine hinreichende Gewähr für die Verarbeitung der Daten unter Einhaltung der in den EU Standardvertragsklauseln 2021 statuierten Pflichten des Auftragnehmers bieten („Zusätzliche Maßnahmen und Zusicherungen“).

Die Verarbeitung der Daten durch den Auftragnehmer darf erst dann beginnen, wenn die in Absatz 2 erwähnten Fragen des Auftraggebers durch den Auftragnehmer beantwortet wurden und die nach Absatz 3 eventuell erforderlichen Zusätzlichen Maßnahmen und Zusicherungen ergriffen bzw. abgegeben wurden.

3. **Verarbeitung durch Unterauftragnehmer im unsicheren Drittland (wenn Auftragnehmer in der EU oder in einem Land mit angemessenem Datenschutzniveau ansässig ist).** Verarbeiten Unterauftragnehmer im Sinne von § 7 Ziffer 1 eines in der EU oder in einem Land mit angemessenem Datenschutzniveau ansässigen Auftragnehmers Daten in einem unsicheren Drittland, stellt der Auftragnehmer in Ergänzung zu den in § 4 Ziffer 1 genannten Voraussetzungen vor Beginn der Verarbeitung durch diese Unterauftragnehmer sicher, dass mit dem Unterauftragnehmer die EU Standardvertragsklauseln 2021 abgeschlossen sind oder dass für den Unterauftragnehmer verbindliche interne Datenschutzvorschriften im Sinne von Art. 47 DSGVO gelten. § 4 Ziffer 2 Absätze 2 und 3 gelten entsprechend im Verhältnis zwischen Auftragnehmer und Unterauftragnehmer. Auf Verlangen des Auftraggebers stellt der Auftragnehmer diesem eine Kopie der insoweit relevanten Dokumente zur Verfügung.

4. **Verarbeitung durch Unterauftragnehmer im unsicheren Drittland (wenn Auftragnehmer nicht in der EU und nicht in einem Land mit angemessenem Datenschutzniveau ansässig ist).** Verarbeiten Unterauftragnehmer im Sinne von § 7 Ziff. 1 eines nicht in der EU und nicht in einem Land mit angemessenem Datenschutzniveau ansässigen Auftragnehmers Daten in einem unsicheren Drittland, schließt der Auftragnehmer in Ergänzung zu den in Ziffer 1 genannten Voraussetzungen vor Beginn der Verarbeitung durch diese Unterauftragnehmer mit diesen vertragliche Vereinbarungen, die in Bezug auf die Verarbeitung durch die Unterauftragnehmer sicherstellen, dass diese Verarbeitung auf einem Datenschutzniveau stattfindet, das dem durch die EU Standardvertragsklauseln 2021 oder durch verbindliche interne Datenschutzvorschriften im Sinne von Art. 47 DSGVO gewährleisteten Niveau entspricht. § 4 Ziffer 2 Absätze 2 und 3 gelten entsprechend im Verhältnis zwischen Auftragnehmer und Unterauftragnehmer. Auf Verlangen des Auftraggebers stellt der Auftragnehmer diesem eine Kopie der insoweit relevanten Dokumente zur Verfügung.

**§ 5 Haftung**

Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend den gesetzlichen Haftungsregelungen (Art. 82 EU DSGVO). Etwaige anderweitig zwischen den Parteien vereinbarte Haftungsbegrenzungen (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung.

**§ 6 Technische und organisatorische Maßnahmen**

1. **Allgemeines.** Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO, insbesondere i. V. m. Art. 5 Abs. 1, Abs. 2 DSGVO, um ein dem sich aus der Verarbeitung der Daten ergebenden Risiko angemessenes Schutzniveau zu gewährleisten.

 Bei der Beurteilung des angemessenen Schutzniveaus berücksichtigen die Vertragsparteien in angemessener Weise den Stand der Technik, die Kosten der Umsetzung, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Risiken für betroffene Personen.

 Vor diesem Hintergrund setzt der Auftragnehmer zumindest die in Anlage 2 definierten technischen und organisatorischen Maßnahmen um.

 Technische und organisatorische Maßnahmen sind Gegenstand technischen Fortschritts und ständiger Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, in Absprache mit dem Auftraggeber, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der vereinbarten technischen und organisatorischen Maßnahmen nicht unterschritten wird. Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen bedürfen der schriftlichen vorherigen Zustimmung durch den Auftraggeber.

2. **Zertifizierung**. Der Auftragnehmer hat darüber hinaus die Eignung zur Umsetzung adäquater Sicherheitsmaßnahmen durch eine entsprechende TISAX oder ISO/IEC 27001-Zertifizierung zu dokumentieren und nachzuweisen.

Der Auftragnehmer ist verpflichtet, die zum Erreichen und Aufrechterhaltung der Zertifizierung erforderlichen Sicherheitsmaßnahmen, die er im Zertifizierungsverfahren angegeben hat, sowie solche Maßnahmen, die in Anlage 2 vertraglich vereinbart wurden, während der gesamten Vertragslaufzeit umzusetzen.

Abweichungen von einer Zertifizierung nach TISAX oder ISO/IEC 27001 sind nur nach vorheriger schriftlicher Zustimmung der zuständigen Stelle der Informationssicherheit des Auftraggebers zulässig.

3. **Prüfrechte**. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

4. **Datenverarbeitung in Privatwohnungen**. Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten in Privatwohnungen ist nur zulässig, wenn auch dort ein angemessenes Sicherheitsniveau in Übereinstimmung mit der DSGVO und dieser Vereinbarung vom Auftragnehmer gewährleistet ist.

**§ 7 Unterauftragnehmer**

1. **Einschaltung von Unterauftragnehmern.** Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen unmittelbar gegenüber dem Auftraggeber und der damit im Zusammenhang stehenden Verarbeitung von Daten Dritte (**„**Unterauftragnehmer**“**) einschaltet, soweit die Anforderungen aus den nachfolgenden Absätzen gewährleistet sind.

 **Zum Zeitpunkt des Vertragsschlusses gestattete Unterauftragnehmer**. Dem Auftragnehmer wird die Einschaltung der in Anlage 1 genannten Unterauftragnehmer gestattet.

1. **Weitere Unterauftragnehmer**. Über beabsichtigte Beauftragungen weiterer Unterauftragnehmer oder Ersetzung bisheriger Unterauftragnehmer ist der Auftraggeber durch den Auftragnehmer unverzüglich, spätestens jedoch 45 Kalendertage vor der Beauftragung, in Schriftform oder per E-Mail zu informieren, damit er ausreichend Zeit hat, um vor der Beauftragung Einwände gegen diese erheben zu können. Der Auftragnehmer stellt dem Auftraggeber dabei die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Die Verarbeitung der Daten durch den Unterauftragnehmer ist erst bei Vorliegen aller gesetzlichen und sich aus diesem Auftragsverarbeitungsvertrag ergebenden Voraussetzungen zulässig.
2. **Verträge mit Unterauftragnehmern.** Der Auftragnehmer muss die von ihm beauftragten Unterauftragnehmer, die Daten verarbeiten, den gleichen vertraglichen Datenschutzpflichten unterwerfen, denen er selbst nach diesem Auftragsverarbeitungsvertrag unterliegt. Der Auftragnehmer überprüft regelmäßig die Einhaltung dieser Datenschutzpflichten durch die Unterauftragnehmer, insbesondere die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen.
3. **Haftung.** Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers.

**§ 8 Kontrollrechte des Auftraggebers**

1. **Kontrollrechte.** Der Auftraggeber hat das Recht, beim Auftragnehmer die Einhaltung der Regelungen dieses Auftragsverarbeitungsvertrages, der erteilten Weisungen und der anwendbaren Datenschutzgesetze selbst oder durch einen vom Auftraggeber benannten geeigneten und zur Verschwiegenheit verpflichteten Dritten zu kontrollieren bzw. kontrollieren zu lassen. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Vor-Ort-Kontrollen und sonstige Überprüfungen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

2. **Unterstützungspflicht.** Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen in einem zumutbaren Umfang unterstützend mitwirkt. Insbesondere gewährt der Auftragnehmer Zugang zu Datenverarbeitungsanlagen, erteilt erforderliche Auskünfte und stellt benötigte Dokumentationen zu Verfügung.

3. **Durchführung.** Kontrollen beim Auftragnehmer sind rechtzeitig anzukündigen und dürfen dessen Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen.

**§ 9 Hinweispflichten**

1. **Rechtswidrige Weisungen.** Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen die EU DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.

2. **Kontrollen durch Aufsichtsbehörden.** Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle Kontrollen und Maßnahmen der Aufsichtsbehörden, soweit die Daten des Auftraggebers betroffen sind. Etwaige festgestellte Beanstandungen der Aufsichtsbehörden wird der Auftragnehmer unverzüglich beheben und dies dem Auftraggeber mitteilen.

3. **Fehler und Unregelmäßigkeiten.** Soweit die Daten des Auftraggebers betroffen sind, teilt der Auftragnehmer dem Auftraggeber unverzüglich Störungen, festgestellte oder vermutete Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen die anwendbaren Datenschutzgesetze oder die im Auftrag getroffenen Festlegungen sowie einen etwaigen Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung der Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach den Art. 33 und 34 DSGVO.

**§ 10 Laufzeit**

1. **Laufzeit.** Die Laufzeit dieses Auftragsverarbeitungsvertrages entspricht der Laufzeit des Hauptvertrages.

2. **Fortgeltung.** Soweit der Auftragnehmer faktisch über die Laufzeit des Hauptvertrages hinaus Daten verarbeitet, z.B. Speicherung aufgrund von Aufbewahrungspflichten, gelten die Vereinbarungen dieses Auftragsverarbeitungsvertrages fort.

**§ 11 Sonstiges**

1. **Änderungen.** Änderungen dieses Auftragsverarbeitungsvertrages bedürfen grundsätzlich der Schriftform, soweit nicht anders in diesem Auftragsverarbeitungsvertrag geregelt.
2. **Anpassungen.** Soweit Anpassungen dieses Auftragsverarbeitungsvertrages erforderlich sind, damit die Parteien die gesetzlichen Vorgaben erfüllen, werden sie die entsprechenden Anpassungen unverzüglich vornehmen.
3. **Kosten.** Die Leistungen des Auftragnehmers nach diesem Auftragsverarbeitungsvertrag sind durch die im Hauptvertrag geregelte Vergütung abgegolten.
4. **Maßnahmen Dritter**. Sind personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, z.B. durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren, oder durch sonstige vergleichbare Ereignisse gefährdet, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
5. **Salvatorische Klausel.** Sollten einzelne Teile dieses Auftragsverarbeitungsvertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht. Auftraggeber und Auftragnehmer verpflichten sich, an Stelle der unwirksamen Regelung eine gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO gerecht wird.

4. **Anwendbares Recht, Gerichtsstand.** Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist der Sitz des Auftraggebers.

5. **Anlagen.** Vertragsbestandteil sind die Anlagen 1 und 2.

Anlage 1 Beschreibung der Auftragsverarbeitung

Anlage 2 Technische und organisatorische Maßnahmen

|  |
| --- |
| **Auftraggeber** |
| Name (in Blockbuchstaben): Klicken oder tippen Sie hier, um Text einzugeben.Funktion / Titel:Klicken oder tippen Sie hier, um Text einzugeben.Ort, Datum:Klicken oder tippen Sie hier, um Text einzugeben.Unterschrift:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Name (in Blockbuchstaben): Klicken oder tippen Sie hier, um Text einzugeben. Funktion / Titel:Klicken oder tippen Sie hier, um Text einzugeben.Ort, Datum:Klicken oder tippen Sie hier, um Text einzugeben.Unterschrift:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Auftragnehmer** |
| Name (in Blockbuchstaben): Klicken oder tippen Sie hier, um Text einzugeben. Funktion / Titel:Klicken oder tippen Sie hier, um Text einzugeben.Ort, Datum:Klicken oder tippen Sie hier, um Text einzugeben.Unterschrift:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Name (in Blockbuchstaben): Klicken oder tippen Sie hier, um Text einzugeben. Funktion / Titel:Klicken oder tippen Sie hier, um Text einzugeben.Ort, Datum:Klicken oder tippen Sie hier, um Text einzugeben.Unterschrift:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Anlage 1

**Beschreibung der Auftragsverarbeitung**

**1. Hauptvertrag**

Hauptvertrag im Sinne von § 1 Ziff. 1 des Auftragsverarbeitungsvertrages:

Titel: ……

Parteien: ……

Datum: ……

**2. Gegenstand der Verarbeitung**

Gegenstand der Verarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

……

**3. Umfang und Zweck der Datenverarbeitung / Datenverarbeitungsmaßnahmen**

Nähere Beschreibung der Verarbeitung im Hinblick auf Umfang und Zweck:

……

**4. Kategorien der betroffenen Personen**

Von der Auftragsverarbeitung sind folgende Personenkreise betroffen:

[ ]  **Mitarbeiter.** Mitarbeiter der eigenen Konzerngesellschaft, d.h. Beschäftigter der verantwortlichen Stelle

*z.B. Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte*

[ ]  **Konzern-Mitarbeiter.** Mitarbeiter einer anderen Konzerngesellschaft, d.h. Beschäftigter einer Gesellschaft des Volkswagen Konzerns, aber nicht der verantwortlichen Stelle

*z.B.: Mitarbeiter anderer MAN Gesellschaften, Scania-Mitarbeiter, Audi-Mitarbeiter*

[ ]  **Partnerfirmen-Mitarbeiter.** Mitarbeiter eines Lieferanten, Dienstleisters, Joint-Ventures, Leiharbeitsfirma

*z.B. Mitarbeiter von Partnerfirmen (z.B. IT-Dienstleister, Zulieferer), Beschäftigte bei Joint-Ventures, Leiharbeitnehmer*

[ ]  **Kunden.** Jede Person, mit der der Auftraggeber in einer Kundengeschäftsbeziehung steht

*z.B. Fahrzeugkäufer, Bankkunden, Versicherungsnehmer, Mietkunden*

[ ]  **Sonstige Geschäftspartner.** Jede natürliche oder juristische Person, mit der der Auftraggeber in einer Geschäftsbeziehung steht, jedoch ohne die Kunden

*z.B. Lieferanten, Importeure oder Servicepartner selbst; Vermittler, Aktionäre, Freelancer*

[ ]  **Außenstehende.** Jede Person, die in keiner Geschäftsbeziehung mit dem Auftraggeber steht

*z.B. Besucher, Gäste, Interessenten*

[ ]  **Kinder.** Die Beurteilung, ob es sich bei einer Person um ein Kind handelt, ergibt sich aus dem jeweiligen Landesrecht.

 *z.B. werden in Deutschland Personen unter 16 Jahren als Kinder bezeichnet*

**5. Kategorien der personenbezogenen Daten**

Die Auftragsverarbeitung umfasst die folgenden Arten personenbezogener Daten:

[ ]  **Berufliche Kontakt- und (Arbeits-)Organisationsdaten**

*z.B. Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Gesellschaft, Bereich, Abteilung, Kostenstelle, Personalnummern, Zuständigkeiten, Funktionen*

[ ]  **IT-Nutzungsdaten**

*z.B. UserID, Rollen, Berechtigungen, Login-Zeiten, Rechnername, IP-Adresse, GID, Legic-Nr.*

[ ]  **Kfz-Nutzungs-Daten mit FIN/Kfz-Kennzeichen - Garantie-, Gewährleistung, Produkthaftung, sicherer Fahrzeugbetrieb.** Bei der Kfz-Nutzung anfallende Daten, die mit FIN/Kfz-Kennzeichen verknüpft sind und im Zusammenhang mit Werkstattreparaturen, Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist.

[ ]  **Private Kontakt- und Identifikationsdaten**

*z.B. Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Geburtsdatum/-ort, Identifikationsnummern, Nationalität*

[ ]  **Vertragsdaten**

*z.B. gekaufte Produkte, (Finanz-)Dienstleistungen, Datum Kaufvertrag, Kaufpreis, Sonderausstattung, Garantien*

[ ]  **Kfz-Nutzungs-Daten mit FIN/Kfz-Kennzeichen - Komforteinstellungen, Multimedia, Navigation.** Bei der Kfz-Nutzung anfallende Daten, die mit FIN/Kfz-Kennzeichen verknüpft sind und Komforteinstellungen betreffen, wie z.B. Sitzeinstellung, bevorzugte Radiosender, Klimaeinstellungen, Navigationsdaten, E-Mail-/SMS-Kontaktdaten.

[ ]  **Kfz-Nutzungs-Daten mit FIN/Kfz-Kennzeichen - Assistenzsysteme, Fahrverhalten etc.** Bei der Kfz-Nutzung anfallende Daten, die mit FIN/Kfz-Kennzeichen verknüpft sind und das Fahrverhalten betreffen bzw. die Nutzung von Assistenzsystemen und deren konkrete Einsatzdaten.

[ ]  **Positionsdaten**

*z.B. GPS, Funknetz-Ortung, Bewegungsprofil, WLAN-Hotspot-Ortung*

[ ]  **Daten zu persönlichen/beruflichen Verhältnissen & Merkmalen**

*z.B. Daten zum Ehegatten oder Kindern, Familienstand, Portraitfoto, Ehrenamt, Berufsbezeichnung, beruflicher Werdegang, Betriebszugehörigkeit, Aufgaben, Tätigkeiten, Eintritts- und Austrittsdaten, Qualifikationen, Bewertungen / Beurteilungen*

[ ]  **Entgelt- und Zeitwirtschaftsdaten**

*z.B. Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe*

[ ]  **Bonitäts- und Bankdaten**

*z.B. Zahlungsverhalten, Bilanzen, Daten von Auskunfteien, Scorewerte, Vermögensverhältnisse, Kontoverbindung, Kreditkartennummer*

[ ]  **Besondere Kategorien personenbezogener Daten**: Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten (Fingerabdruck, Spracherkennung, Iris-Scan, etc.), Daten über Gesundheit, Daten über Sexualleben oder sexuelle Orientierung.

 Nur für den Fall, dass besondere Kategorien personenbezogener Daten in unsicheren Drittländern verarbeitet werden:

a) Bitte hier die einschlägigen besonderen Kategorien personenbezogener Daten konkret angeben:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b) Bitte hier die in Bezug auf die unter a) genannten besonderen Kategorien personenbezogener Daten vereinbarten Beschränkungen und Garantien angeben, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, z.B. strenge Zweckbindung, Zugangsbeschränkungen, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  **Personenbezogene Daten über Straftaten / Ordnungswidrigkeiten:** Daten, die sich auf strafbare Handlungen oder den Verdacht auf solche beziehen.

[ ]  **Sonderkategorie: Mitarbeiterfoto.** Portraitfoto, das durch den Mitarbeiter auf freiwilliger Basis veröffentlicht wird (z.B. Intranet-Telefonbuch, interne Social-Media-Plattform)

**6. Weitere Beschreibung der Datenübermittlung**

Wenn die EU Standardvertragsklauseln 2021 Vertragsbestandteil sind, bitte hier weitere Informationen angeben:

a) Häufigkeit der Übermittlung der Daten in Unsichere Drittländer (Mehrfachauswahl möglich):

 [ ]  einmalig [ ]  regelmäßig [ ]  kontinuierlich

b) Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Mehrfachauswahl möglich):

[ ]  Keine bzw. nur flüchtige Speicherung

[ ]  Speicherung bis zur Erreichung des individuellen Verarbeitungszwecks

[ ]  Speicherung bis zur Beendigung des Hauptvertrages

Ggf. Kriterien für die Festlegung der Dauer:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­\_\_\_\_\_\_\_\_\_­\_

c) Zuständige Aufsichtsbehörde

 Für den Auftraggeber zuständige Aufsichtsbehörde:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**7. Spezielle Weisungen bei Vertragsbeginn**

[ ]  Anonymisierung bestimmter Daten: …

[ ]  Verbot der Weitergabe von Daten: …

[ ]  Löschung der Daten nach jeweils … Monaten

[ ]  Folgende Richtlinien, Handbücher und Betriebsvereinbarungen sind zu beachten: …

[ ]  …

**8. Ort der Verarbeitung** *Mehrfachnennungen möglich!*

[ ]  Deutschland

[ ]  Mitgliedsstaat der Europäischen Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum

Belgien, Bulgarien, Dänemark, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn, Zypern

Island, Norwegen, Liechtenstein

[ ]  Länder mit angemessenem Datenschutzniveau, derzeit:

Andorra, Argentinien, Australien (Nur eingeschränkt für Flugpassagierdaten), Färöer Inseln, Guernsey, Isle of Man, Israel, Japan, Jersey, Kanada, Neuseeland, Schweiz, Südkorea,
Uruguay, Vereinigtes Königsreich (UK), Vereinigte Staaten von Amerika (USA; nur bei vorliegender Zertifizierung nach dem EU-U.S. Data Privacy Framework).

[ ]  Unsicheres Drittland: ..…

Wenn eine Datenverarbeitung in einem unsicheren Drittland stattfindet, muss zumindest eine der nachstehend genannten zusätzlichen Zulässigkeitsvoraussetzungen gegeben sein. Bitte kreuzen Sie alle zutreffenden Alternativen an.

[ ]  Zwischen dem Auftraggeber und jedem Auftragnehmer in einem unsicheren Drittland ist Modul 2 der EU Standardvertragsklauseln 2021 abgeschlossen.

[ ]  Zwischen dem Auftragnehmer und jedem Unterauftragnehmer in einem unsicheren Drittland ist Modul 3 der EU Standardvertragsklauseln 2021 abgeschlossen.

[ ]  Die Datenverarbeitung ist durch eine Einwilligung der betroffenen Personen gedeckt.

[ ]  Für den Auftragnehmer und jeden Unterauftragnehmer gelten verbindliche interne Datenschutzvorschriften im Sinne von Art. 47 DSGVO (Binding Corporate Rules).

**9. Weisungs- und Kontrollberechtigte beim Auftraggeber**

Name: ……

Kontaktdaten (E-Mail, Telefon, Anschrift): ……

**10. Zuständige Weisungsempfänger beim Auftragnehmer**

Name: ……

Kontaktdaten (E-Mail, Telefon, Anschrift): ……

**11. Datenschutzbeauftragter bzw. Ansprechpartner Datenschutz des Auftragnehmers**

 Der Auftragnehmer hat folgenden Datenschutzbeauftragten bestellt:

 Name: ……

 Kontaktdaten (E-Mail, Telefon, Anschrift): ……

 Der Auftragnehmer hat folgenden Ansprechpartner Datenschutz ernannt:

 Name: ……

 Kontaktdaten (E-Mail, Telefon, Anschrift): ……

**12. Unterauftragnehmer**

[ ]  Der Auftragnehmer setzt keine Unterauftragnehmer ein.

[ ]  Der Auftragnehmer setzt folgende Unterauftragnehmer ein:

Nr. \_\_ Unterauftragnehmer (Name, Rechtsform, Adresse, Ansprechpartner):

...

Verarbeitete Datenkategorien:

...

Verarbeitungstätigkeit des Unterauftragnehmers (stichwortartige Beschreibung der Aufgaben):

...

Dauer der Verarbeitung:

...

Die Verarbeitung erfolgt (auch) in folgenden unsicheren Drittländern:

...

**13. Meldung von Datenschutzverletzungen**

Die Meldung von Datenschutzverletzungen des Auftragnehmers erfolgt an die nachfolgend ausgewählten Funktions-E-Mail-Postfächer des Auftraggebers:

[ ]  DSGVO-Zentralteam@man.eu

[ ]  mtb-iso@man.eu

[ ]  mtb-cdc@man.eu

[ ]  information-security@traton.com

[ ]  ...

**14. Datenverarbeitung in Privatwohnungen**

[ ]  Ja, es findet eine Datenverarbeitung in Privatwohnungen statt.

[ ]  Nein, es findet keine Datenverarbeitung in Privatwohnungen statt.

Anlage 2

**Technische und organisatorische Maßnahmen**

1. Der Auftragnehmer hat die folgenden technischen und organisatorischen Maßnahmen getroffen:

…Liste der TOMs…

bzw.

Verweis auf ein Datensicherheitskonzept gemäß Art. 32 DS-GVO

1. Der Auftragnehmer weist seine Eignung durch Vorlage der nachfolgend angegebenen Zertifizierungen nach

[ ]  VDA ISA (TISAX Label - mit dem Auftraggeber in der ENX Datenbank geteilt)

[ ]  ISO 27001 – Zertifikat (inklusive Statement of Applicability)

Weitere vorhandene Zertifizierungen: (zusätzlich zu den oben genannten Grundanforderungen):

[ ]  Cloud Vendor Assessment (DCSO)

[ ]  BSI C5 (Bundesamt für Sicherheit in der Informationstechnik, Cloud)

[ ]  CSA STAR (Cloud Security Alliance)

[ ]  ISO 27017 (Erweiterung von ISO 27001 in Bezug auf Cloud Controls)

[ ]  ISO 27018 (Erweiterung von ISO 27001 in Bezug auf personenbezogene Daten)