Vereinbarung zur Auftragsverarbeitung DS-GVO

zwischen

Verantwortlicher

Besteller gemäß Einzelauftrag über "Vehicle Management Solution"

- nachstehend Auftraggeber genannt -

und

Auftragsverarbeiter

ETAS GmbH
Borsigstraße 24
70439 Stuttgart

- nachstehend Auftragnehmer genannt -

Präambel

Diese Vereinbarung legt die Verpflichtungen der Vertragsparteien zum Datenschutz fest, die sich aus der Beauftragung von *"Vehicle Management Solution"* (nachfolgend „Vertrag") in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag 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, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Gegenstand der Auftragsverarbeitung ist im Vertrag beschrieben. Im Wesentlichen handelt es sich um folgende Aufgaben durch den Auftragnehmer:

- *Betrieb eines Telematik Dienst der ein Connectivity Steuergerät sowie Backend Dienste inkludiert zur Verfügungsstellung von Fahrzeuginformationen wie beispielsweise technische Messdaten oder Diagnosedaten eines Kundenfahrzeugs.*
- *Verfügung Stellung von Updatefähigkeit über Mobilfunk (over-the-air update).*
- *Exportfunktionalität der gesammelten Daten auf Kundenwunsch*

1.2 Art und Zweck der Auftragsverarbeitung sind im Vertrag beschrieben und umfassen insbesondere:

- *Bereitstellung von Fahrzeug Mess- und Diagnosedaten.*
- *Speicherung der Fahrzeug Mess- und Diagnosedaten für einen definierten Zeitraum*
- *Identitäts und Zugriffsverwaltung der Nutzer*

1.3 Die Verarbeitung umfasst die nachfolgend genannten Kategorien von Daten:

☒ persönliche Angaben: *email-Adresse, Name*

☒ Logging-Daten / Protokolle: IP-Adresse, Meta-Daten

☒ Sonstiges:

Meta-Daten:

Beschreibung der Fahrzeugkonfiguration wie beispielsweise Connectivity Steuergeräte ID, Fahrzeugidentifikationsnummer und Softwarestand der im Fahrzeug installierten Steuergeräte.

Technische Messdaten eines Fahrzeugs: Technische Signale die im Fahrzeugnetzwerk verfügbar sind wie beispielsweise Geschwindigkeit, Druck und Drehzahl.

Technische Daten des Connectivity Steuergeräts: Betriebsrelevante Daten wie Log-Daten, Netzwerkverbindungsinformationen

Technische Diagnosedaten eines Fahrzeugs: Diagnoseinformationen wie beispielswesie Fehlercodes des Fahrzeugs.

Positionsinformationen des Fahrzeugs

1.4 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:

☒ Personal einschließlich Freiwilliger, Beauftragte, Zeitarbeitskräfte und Aushilfen.

☒ Verwandte, Erziehungsberechtigte, Angehörige, Gutachter, Treuhänder und andere Personen, die mit der betroffenen Person in Verbindung stehen.

☒ Kunden und Auftraggeber

1.5 Die Laufzeit dieser Vereinbarung und die Dauer der Verarbeitung richten sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

1.6 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau im Drittland:

☒ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☒ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c) und d) DS- GVO);

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist hinsichtlich der

Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Einzelweisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und der Auftragnehmer darf hierfür eine angemessene Vergütung verlangen.

2.3 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform..

2.4 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstößt gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf personenbezogene Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin, soweit das betreffende Recht einen Hinweis nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die in **Anhang 1** beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer gewährleisten. Dem Auftraggeber sind diese technischen und organisatorischen

Maßnahmen bekannt. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch gewährleistet sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten. Hierfür kann der Auftragnehmer eine angemessene Vergütung verlangen.

3.5 Der Auftragnehmer gewährleistet, dass es seinen mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- oder Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DS-GVO zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Sofern der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, nennt er dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Erster Ansprechpartner in Datenschutzfragen:
Name: Beate Winter
Anschrift: Borsigstrasse 24, 70469 Stuttgart
E-Mail: beate.winter@etas.com
Telefonnummer:+49(711)3423–2679

Sowie die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:
Name: Thoralf Knuth, Datenschutzbeauftragter, Abteilung Informationssicherheit und Datenschutz der Bosch Gruppe (C/ISP)
Anschrift: Kronenstrasse 22 – 26, 70173 Stuttgart
E-Mail: DPO@bosch.com

3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und 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 personenbezogenen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Beschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart.

3.10 Die personenbezogenen Daten werden nach dem Ende des jeweiligen Vertrages gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen personenbezogenen Daten anzufertigen und die personenbezogenen Daten vor Vertragsende umzuziehen. Eine Pflicht des Auftragnehmers zur Herausgabe von personenbezogenen Daten, auf die der Auftraggeber selbst Zugriff hat, besteht nicht.

3.11 Der Auftragnehmer verpflichtet sich zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO.

4. Pflichten des Auftraggebers

4.1 Dem Auftraggeber obliegt es, dem Auftragnehmer die personenbezogenen Daten rechtzeitig zur Leistungserbringung nach dem Vertrag zur Verfügung zu stellen. Er ist für die Qualität der personenbezogenen Daten verantwortlich. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Leistungen feststellt.

4.2 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichten sich Auftraggeber und Auftragnehmer, sich bei der Abwehr des Anspruches gegenseitig zu unterstützen.

4.3 Bitte teilen Sie uns bei Auftragserteilung Ihren Ansprechpartner für die im Rahmen der Verarbeitung anfallenden Datenschutzfragen mit sowie ggf. die Kontaktdaten des Datenschutzbeauftragten des Auftraggebers. Falls Sie uns keinen anderweitigen Ansprechpartner nennen, werden wir den „Cloud Administrator des Kunden“ informieren.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder Auskunft über die personenbezogenen Daten an den Auftragnehmer, wird er dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber auf Anfrage die Einhaltung der in Art. 28 DS-GVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer dem Auftraggeber Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DS-GVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten oder von diesen beauftragten Personen.

6.2 Sollten im Einzelfall Kontrollen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten Montag – Freitag zwischen 08:00 Uhr und 17:00 Uhr ohne Störung des Betriebsablaufs und nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mind. 4 Tagen durchgeführt. Der Auftragnehmer darf die Kontrollen von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung durch den Auftraggeber oder den von diesem beauftragen Prüfer abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Widerspruchsrecht. Der Widerspruch ist in Textform gegenüber dem Auftraggeber zu erklären.

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Kontrolle vornehmen, gilt grundsätzlich 6.2 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.

6.4 Für die Unterstützung bei der Durchführung einer Kontrolle nach 6.2 oder 6.3 darf der Auftragnehmer eine angemessene Vergütung verlangen, sofern nicht Anlass der Kontrolle der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmers ist. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Kontrolle vom Auftraggeber vorzutragen.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber direkt in Textform oder über den Internetauftritt des Auftragnehmers (www.etas.com/AGB-ETASGmbH) mit einer Frist von vier Wochen vorab. Der Auftraggeber kann der Hinzuziehung oder Ersetzung nur aus wichtigem Grund widersprechen. Der Widerspruch hat schriftlich binnen 14 Tagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Hinzuziehung oder Ersetzung als gegeben. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung des

Auftrages beseitigt werden kann, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Über die in **Anhang 2** aufgeführten, bei Vertragsschluss bereits hinzugezogenen, Subunternehmer und deren Teilleistungen erfolgt keine gesonderte Information. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

7.2 Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

7.3 Die Regelungen in dieser Ziffer 7 gelten auch, wenn – unter Wahrung der Grundsätze von Kapitel 5 der DS-GVO – ein Subunternehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Kapitel 5 der DS-GVO im erforderlichen Maße mitzuwirken.

8. Haftung

8.1 Neben den gesetzlichen Haftungsbeschränkungen gelten die Haftungsbeschränkungen aus dem Vertrag.

8.2 Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer aufgrund der vom Aufraggeber beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer weisungswidrigen Verarbeitung der personenbezogenen Daten durch den Auftragnehmer beruht.

9. Informationspflichten, Schriftformklausel, Rechtswahl

9.1 Sollten die personenbezogenen 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 Dritten in diesem Zusammenhang unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-GVO liegt.

9.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

9.4 Gerichtsstand ist Stuttgart.

Anhang 1: Technisch-organisatorische Maßnahmen / Sicherheitskonzept

Vertraulichkeit (Artikel 32 Paragraph 1 lit b DSGVO)

Physische Zugangskontrolle
Verhinderung des Zugriffs unberechtigter Personen auf Systeme zur Verarbeitung personenbezogener Daten.

- Definition von Personen mit Zugangsberechtigung
- Dokumentierte Vorschriften für die Zugangskontrolle
- Bedarfsgerechte Zugriffsrechte
- Zugangskontrolle mit personalisiertem und verschlüsseltem Ausweis mit Foto
- Verpflichtung, jederzeit einen Ausweis mitzuführen
- Magnet- oder Chipkarten
- Protokollierung des Zugriffs auf Serverräume (automatisch durch Zugriffskontrollsystem oder durch entworfene Listen)
- Biometrische Zugangskontrolle (zum Beispiel zu Serverräumen)
- Restriktive Regeln für Schlüssel
- konventionelles Schließsystem (Stationsschlüssel)
- Verschiedene Sicherheitszonen
- Protokollierung von Systemzugriffsereignissen
- Besucher auf dem Gelände nur in Begleitung von Mitarbeitern des Vertragsdatenverarbeiters gestattet
- Sicherheitspersonal
- Türstatusüberwachung für Serverraum
- Baumaßnahmen (z. B. einbruchhemmende Fenster)
- Dokumentation der Vergabe oder des Widerrufs von Zugriffsberechtigungen
- Berechtigungskonzept
- Etablierte Kontrollmechanismen (z. B. stichprobenartig dokumentierte Vorschriften für die Zugangskontrolle der Schlüsselverwaltung)
- Bestimmungen für den Zugang externer Personen
- Das Tragen von Berechtigungskarten ist obligatorisch
- Identitätskontrolle am Empfang
- Zusätzliche Maßnahmen zur Zugangskontrolle und Überwachung des Status von Türen, die zu Servereinrichtungen führen
- Sicherheitsschlösser
- Videoüberwachung in Serverräumen
- Videoüberwachung von Eingangsbereichen
- Videoüberwachung der Datencenter
- Anlagensicherheitsdienste
- Überwachung von Notausgängen
- Automatische Türzuziehvorrichtung zum Ein- und Austritt in Serverräumen
- Alarm Systeme / Intrusion Detection System
- Einbruchsicherungssysteme mit direkter Alarmierung einer ständig besetzten Sicherheitszentrale oder einer Polizeistation

.Logische Zugangskontrolle
Verhinderung der unbefugten Nutzung personenbezogener Datenverarbeitungssysteme.

- Passwortrichtlinie (sichere / komplexe Passwörter)
- Passwortbestimmungen (z. B. Bestimmungen zur Verwendung von Sonderzeichen, Mindestlänge, regelmäßige Änderung des Passworts)
- Standardeinstellungen der zu verwendenden Kennwortverwaltungsanwendungen
- Authentifizierung mit Benutzername / Passwort
- Verbot der Weitergabe von Passwörtern
- Sperrung bei falschen Zugriffsversuchen
- Regelmäßige Passwortänderung
- regelmäßige Überprüfung der Zugriffsberechtigungen
- Aufgabentrennung bei der Vergabe von Benutzerrechten
- Sperrung von Workstation- und / oder Benutzerkonten nach mehrfachen fehlerhaften Anmeldungen
- Regelmäßige Zugriffsberechtigungen prüfen den Benutzerzugriff auf das Netzwerk der Mitarbeiter und Externen
- Automatisches Sperren des Bildschirms bei Inaktivität nach einiger Zeit
- Isolierung interner Netzwerke durch Einrichtung von Firewall-Systemen
- Regelmäßige Zugriffskontrollen für Administratoren von Netzwerken, Netzwerkdiensten, Servern und Anwendungen, bei denen das Risiko erkannt wurde
- Segmentierung von Netzwerken
- Verwendung von virtuellen privaten Netzwerken (VPN) mit Benutzer / Passwort als Authentifizierungskriterium und / oder Token zur Authentifizierung
- Verschlüsselte Smartphones
- Abschotten interner Netzwerke durch Installation von Firewall-Systemen
- Intrusion-Detection-System
- Verschlüsselung von mobile Endgeräten (z.B. Laptops)
- Anti-virus Software (Client / Server)
- Hardware Firewall
- Software Firewall

Datenzugriffskontrolle
Gewährleistung, dass Personen, die zur Nutzung eines personenbezogenen Datenverarbeitungssystems berechtigt sind, nur Zugang zu solchen personenbezogenen Daten erhalten, auf die sie gemäß ihren Zugriffsrechten zugreifen dürfen, und dass personenbezogene Daten während der Verarbeitung oder Nutzung und anschließenden Speicherung nicht gelesen werden können, ohne Genehmigung kopiert, geändert oder gelöscht werden können.

- Verwendung individueller und benutzerbezogener Berechtigungsinformationen
- Definierte Berechtigungskonzepte
- Protokollierung erteilter Berechtigungen
- Dokumentation der Berechtigungsvergabe
- Datenschutzgerechte Entsorgung von Daten, Datenträgern und Ausdrucken nach dem Sicherheitskonzept
- Anzahl der Administrationen auf das Notwendigste begrenzt
- Regelmäßige Kontrolle der Benutzerrechte
- Protokollierung des Zugriffs auf vertrauliche Daten
- Löschen von Daten vor Wiederverwendung von Datenträgern
- Sperrung externer Schnittstellen

Trennungskontrolle
Sicherstellen, dass für verschiedene Zwecke erhobene personenbezogene Daten getrennt verarbeitet werden können.

- Logische / technische Datentrennung oder interne Mandantenfähigkeit
- Zugriffsberechtigungen
- Logische Client-Datentrennung
- Trennung von Entwicklungs-, Test- und Produktionssystemen

Pseudonymisierung
Trennung von Daten von direkten Identifikatoren, so dass eine Verknüpfung mit einer Identität nicht möglich ist, ohne zusätzliche Informationen, die vom Kunden separat gespeichert werden.

- Pseudonomisierte Identitäten für den Plattformbetreiber
- Vom Kunden pseudonymisierte Daten können in Systemen gespeichert werden. Bosch kann die Daten nicht mit bestimmten Daten verknüpfen vorbehaltlich der Unterstützung von zusätzlichen Daten des Kunden

Verschlüsselung
Maßnahmen zum Schutz der Daten vor der Verarbeitung durch unbefugte Personen

- Verschlüsselung vertraulicher Daten während des Transports und über Datennetze
- Bei den Verschlüsselungsrichtlinien werden die verschiedenen Schutzkategorien für personenbezogene
- Schulung interner und externer Mitarbeiter im Umgang mit verschlüsselten personenbezogenen Daten
- Verwendung der Datenverschlüsselung während der Datenübertragung zum Rechenzentrum (falls vom Kunden

Daten berücksichtigt

implementiert)

- Anweisungen zur Verwendung koordinierter und genehmigter kryptografischer Techniken, Algorithmen, Anwendungen und Standards
- Geheimhaltung der privaten Schlüssel eines Zertifikats
- Regelmäßige Überprüfung der Verschlüsselungsprozesse (insbesondere auf Sicherheitslücken) und Anpassung dieser Prozesse an die aktuellen technologischen Entwicklungen (insbesondere Aktualisierung der verwendeten Software)
- Sichere Datenübertragung (SFTP, VPN, TLS)
- Löschen oder Zerstören von Schlüsseln, die nicht mehr auf sichere Weise benötigt werden

Integrität (Artikel 32 Paragraph 1 lit b DSGVO)

Datenübertragungskontrolle
Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten während der elektronischen Übertragung oder des Transports

- Verwendung von virtual private networks (VPN)
- Datenschutzgerechte Entsorgung von Daten, Datenträgern und Ausdrucken nach dem Sicherheitskonzept
- Dokumentation der Vergabe von Berechtigungen und Rollen
- Dokumentation der Hard- und Software im Inventar und Führen eines Inventarregisters
- Elektronische Signatur
- Sichere Datenübertragung (SFTP, VPN, TLS)
- Verwendung der Datenverschlüsselung während der Datenübertragung zum Rechenzentrum
- Beschränkung der zur Übertragung berechtigten Personengruppe
- Kontrollierte Zerstörung von Datenträgern durch zertifizierte Entsorgungsunternehmen

Eingabekontrolle
Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben werden, wird geändert oder gelöscht

- Rechtsform von Verträgen zur Datenverarbeitung personenbezogener Daten mit Subprozessoren, einschließlich geeigneter Vorschriften für Kontrollmechanismen
- Beschaffung von Selbstauskünften von Dienstleistern im Hinblick auf deren Umsetzung des Datenschutzgesetzes

Verfügbarkeit und Belastbarkeit (Artikel 32 Paragraph 1 lit b DSGVO)

Verfügbarkeit
Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Zentraler Einkauf von Software und Hardware
- Zentrale Beschaffung von Hard- und Software
- Sicherungsstrategie (online / offline; vor Ort / außerhalb des Standorts)
- Regelmäßige Datensicherung oder Verwendung von Redundanzen
- Unterbrechungsfreie Stromversorgung in Serverräumen
- Brandschutztüren
- Brand- / Rauchfrüherkennungssysteme
- Alarm System in Serveräumen
- Geschäftskontinuitätsplanung
- Notfallplan
- Mehrschichtige Antivirus- und Firewall-Architektur
- Virusschutz
- Meldeverfahren
- Regelmäßige Datensicherung oder Spiegelung von Festplatten, z. RAID-Verfahren
- Datensicherheitskonzept mit regelmäßigen Backups
- Redundante Speicherung personenbezogener Daten
- Betrieb und regelmäßige Überprüfung der unterbrechungsfreien Stromversorgung (USV), der Notstromversorgung und des Überspannungsschutzes
- IT-Überwachung durch qualifizierte Mitarbeiter, die kontinuierlich geschult werden
- Frühwarnsystem für Feuer, Wasser und hohe Temperaturen in Serverräumen
- Aufbewahrung von Datenträgern in verschiedenen Brandbereichen
- Feuerlöscher in Serverräumen
- Klimatisierung in Serverräumen
- Zwei unabhängige Arten des Zugriffs auf das externe Netzwerk (Internetzugang über mindestens zwei verschiedene Anbieter)
- Verfügbarkeit von Backup-Computern und Softwarelösungen für Notfälle
- Firewall

Belastbarkeit
Maßnahmen zur Sicherstellung einer dauerhaften Belastbarkeit der Systeme und Dienste

- Load-Balancing
- Regelmäßige Schulung des eingesetzten Personals (sowohl des Managements als auch anderer interner oder externer Mitarbeiter) zur Einhaltung der Anforderungen an die Integrität und Vertraulichkeit der Datenverarbeitung (mindestens einmal im Jahr)
- Penetration tests

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Artikel 32 Paragraph 1 lit d DSGVO; Artikel 25 Paragraph 1 DSGVO)

Datenschutzmanagement
Gewährleistung der Rechtmäßigkeit, Angemessenheit und Wirksamkeit des Datenschutzes

- Interne Audits durch die zuständigen Behörden (z. B. Auditoren, Datenschutzbeauftragte, Informationssicherheitsbeauftragte, Prozesskontrollen durch Qualitätsmanagement)
- Externe Audits durch Auditoren, Zertifizierungsstellen in Bezug auf ISO 27001
- Aufbau einer Datenschutzorganisation und eines Datenschutzmanagements
- Datenschutzkonzepte
- Datenschutzschulungen für Mitarbeiter
- Kommunikationskanal für Sicherheitsvorfälle
- Interne und externe Testberichte und Bewertungen
- Benennung des Datenschutzbeauftragten
- Interne Datenschutzprüfungen

Kontrolle der Einhaltung von Anweisungen
Sicherstellen, dass personenbezogene Daten ausschließlich in Übereinstimmung mit den Anweisungen verarbeitet werden.

- Vertragliche Vereinbarung über Aufsichts- und Prüfungsrechte des für die Verarbeitung Verantwortlichen
- Ausführliche schriftliche Regelungen (Vertrag / Vereinbarung) des Auftragsverhältnisses und Formalisierung des gesamten Auftragsablaufs einschließlich des Einsatzes von Subprozessoren, klare Regelungen zu Kompetenzen und Verantwortlichkeiten
- Vertragliche Vereinbarung mit Subprozessoren, dass sowohl internes als auch externes Personal zur Geheimhaltung von Daten verpflichtet wird
- Due Diligence bei der Lieferantenauswahl
- Der Auftragnehmer hat einen Datenschutzbeauftragten ernannt
- Verpflichtung der Mitarbeiter des Auftragnehmers zum Datengeheimnis

Anhang 2: Subunternehmer des Auftragnehmers

	Name, Anschrift des Subunternehmens	Auftragsinhalt	Ort der Datenverarbeitung
1.	Robert Bosch GmbH Connected Mobility Solutions	Organisation des Kunden-Supports Sowie Bereitstellung eines IT-Systems inklusive eines Cloud-Dienstes über den Corporate Sector Information Systems & Services	Hoferstraße 30 71636 Ludwigsburg
2.	Bosch (South East Asia) Pte. Ltd	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	11 Bishan Street 21 (Opposite Raffles Institution), Singapore 573943
3.	Robert Bosch Engineering and Business Solutions Private Limited	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	No. 123 Industrial Lay- out Hosur Road, 560095 Bengaluru, India
4.	Bosch (China) Investment Ltd.	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung	333 Fuquan Road North, Changning District, China

		gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	
5.	Robert Bosch Ltda.	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	Via Anhanguera Km 98- Bairro Boa Vista - Cl, Campinas - SP - CEP : 13065-900, Sao Paulo, Brazil
6.	Robert Bosch North America LLC	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	38000 Hills Tech Drive, Farmington Hills, MI 48331, USA
7.	Robert Bosch Tool Corporation	Bereitstellung eines IT-Service im Bereich der "BIC-Services" (Bosch Internet of Things Cloud-Service) einschließlich, aber nicht beschränkt, auf „Software as a Service", „Platform as a Service" sowie Infrastruktur als Service. Dies beinhaltet das Hosting, Überwachung, Change-Management sowie Problem- und Störungsbehebung. Des Weiteren beinhaltet dies die Dokumentation aller Betriebsabläufe aller Dienste, Anwendungen und IT-Infrastrukturen die dem Data Controller innerhalb des BIC-Services zur Verfügung gestellt werden. Hierbei kann der Zugriff auf personenbezogene Daten zumindest nicht ausgeschlossen werden.	1800 West Central Road, IL60056 Mount Prospect, USA
8.	EMC Deutschland GmbH	Services auf infrastruktureller Ebene (Betriebssystem- und „near-operativ-system" Services); Services, die VMware-Produkte verwenden. Dies umfasst die Virtualisierungsplattform auf System- und Netzwerkebene, Überwachungs- und	Am Kronberger Hang 2A, 65824 Schwalbach am Taunus, Germany

		Dokumentationssysteme sowie Automatisierungssysteme; automatisierte Prozesse, die innerhalb des Automatisierungssystems implementiert wurden. Mit diesen Prozessen können BIC-Kunden (Bosch Internet of Things Cloud-Services) automatisierte virtuelle Windows- und Linux-Systeme und -Dienste auf Plattformebene bereitgestellt werden. Dies umfasst die Laufzeitumgebung (Cloud Foundry) und die Basisdienste, die den Kunden der BIC auf dem Markt zur Verfügung gestellt werden. Der Betrieb der Dienste / Prozesse umfasst: Überwachung, Änderungsmanagement und Fehlerbehebung sowie, falls erforderlich, Dokumentation von Betriebsabläufen und Verfahrensanweisungen in Betriebshandbüchern (Runbooks), wobei die Möglichkeit des Zugriffs auf personenbezogene Daten des für die Verarbeitung des Datenverwalters zumindest nicht ausgeschlossen werden kann.	
9.	Microsoft Deutschland GmbH	Technischer Support für Microsoft Software im Zusammenhang mit Active Directory, die zum Einrichten und Betreiben der BIC-Dienste verwendet werden, wobei die Möglichkeit des Zugriffs auf personenbezogene Daten des Datenverwalters zumindest nicht ausgeschlossen werden kann.	Konrad-Zuse-Strasse 1, 85716 Unterschleissheim, Germany
10.	retarus GmbH	Technische Unterstützung von Retarus Software im Zusammenhang mit Mailingdiensten, die zum Einrichten und Betreiben der BIC-Dienste verwendet werden, wobei die Möglichkeit des Zugriffs auf personenbezogene Daten des Data-Controllers zumindest nicht ausgeschlossen werden können.	Aschauer Strasse 30, 81549 München, Germany
11.	Bosch.IO GmbH (früher Bosch Software Innovations GmbH)	Dienstleistung im Bereich des Betriebs von BIC-Services (Bosch Internet of Things Cloud-Services), insbesondere Software als Service, Plattform als Service und Infrastruktur als Service. Überwachung, Änderungsmanagement sowie Fehlerbehebung und Dokumentation von Betriebsprozessen für alle vom Datenverantwortlichen bereitgestellten oder gegebenenfalls genutzten Dienste oder Anwendungen und IT-Infrastrukturen, wobei die Möglichkeit des Zugriffs auf personenbezogene Daten zumindest nicht ausgeschlossen werden kann.	Ullsteinstraße 128, 12109 Berlin