B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Nutzungsbedingungen für autorisierte Servicepartner in Bezug auf das B2B Connect Seller Center und den WebParts-Händler-Client

zwischen Mercedes-Benz AG, Mercedesstraße 120, Stuttgart (im Folgenden "**MBAG**" genannt) und dem autorisierten Servicepartner (im Folgenden "**Partner**" genannt) von Mercedes-Benz AG, der B2B Connect und verbundene Services nutzt (B2B Connect Seller Center und WebParts-Händler-Client im Folgenden zusammen "**B2B Connect**" genannt).

Kunden in diesem Zusammenhang sind unabhängige Business-to-Business-Unternehmer, die Reparatur- und Wartungsdienstleistungen für Kraftfahrzeuge erbringen (z. B. einzelne Dienstleister und Flottenkunden) (im Folgenden auch als **"Kunde**" bezeichnet).

Mercedes-Benz AG und Partner werden im Folgenden auch als "**Vertragspartner**" bezeichnet.

Präambel

B2B Connect wird von Mercedes-Benz AG bereitgestellt. B2B Connect ist ein technisches Ökosystem, das sowohl den Mercedes-Benz Originalteilevertrieb über das B2B Connect Seller Center (wie im Mercedes-Benz Aftersales-Ökosystem verfügbar) als auch Kunden über andere Subsysteme angebotene Reparatur- und Wartungslösungen integriert, soweit diese im betreffenden Markt verfügbar sind. Partnern werden Services rund um B2B Connect über den WebParts-Händler-Client und das B2B Connect Seller Center angeboten. Features des WebParts-Händler-Client werden zum B2B Connect Seller Center migriert.

Der Kunde erhält den Zugang zu B2B Connect durch Selbstregistrierung und kann seine Daten selbst anpassen, jedoch ist die Online-Bestellung von Mercedes-Benz Originalteilen über B2B Connect für den Kunden erst nach der Annahme und Freischaltung durch den Partner im WebParts-Händler-Client verfügbar (auch nach der Migration zum B2B Connect Seller Center).

Ziel des aktuellen WebParts-Händler-Client und des B2B Connect Seller Centers ist es, dem Partner eine kundenorientierte, systemische Lösung im Internet als Marketinginstrument im After-Sales (Thekengeschäft) zur Verfügung zu stellen sowie die Steigerung der Wettbewerbsfähigkeit und Rentabilität im After-Sales-Geschäft zu ermöglichen. Die Bestimmungen im Kundendienst- und Teilevertriebsvertrag gelten auch für diese Nutzungsbedingungen.

Die Kundendaten für den Bestellvorgang werden dem Partner über den WebParts-Händler-Client und in Zukunft über das B2B Connect Seller Center angezeigt und können in das Verwaltungssystem des Partners importiert werden.

§ 1 Systemvoraussetzungen

Um dem Kunden die Teileverfügbarkeit des Partners anzuzeigen, muss der Partner an den Logistikbus angeschlossen sein, der von der MBAG bereitgestellt wird. Ansonsten ist die Verfügbarkeit von Informationen begrenzt.

§ 2 Mercedes-Benz AG Dienstleistungen, Vertragsabschlüsse, Änderung, Beteiligung und 5*Rater

Mercedes-Benz AG B2B stellt dem Partner das B2B Connect Seller Center und den WebParts-Händler-Client zur Verfügung, die die Online-Bestellung von Originalteilen für Kunden des Partners ermöglichen.

B2B Connect Seller Center und WebParts-Händler-Client, die von Mercedes-Benz AG bereitgestellt werden, ermöglichen es dem Partner:

- die aktivierten Kunden zu sehen,
- die Listenpreise anzupassen,
- Rabattsätze zu definieren,
- eigene Kundenrabatt-Codes zu definieren,
- den ausgewählten Kundenrabattcode zuzuweisen,
- eigene Rabattgruppen zu definieren,
- Informationen zum Support von Kundenanfragen hinsichtlich des voraussichtlichen Lieferzeitpunkts festzulegen,
- von Kunden über den 5*Rater Rückmeldungen zu seinen Produkten, Dienstleistungen und seiner Gesamtleistung zu erhalten sowie
- maßgeschneiderte Kampagnenvorschläge und Kampagnenunterstützungsdienste auf der Grundlage von Informationen zu Transaktionen zu erhalten, die über B2B Connect mit Kunden durchgeführt wurden (d. h. Kundenname, auftragsbezogene Informationen usw.)
- Bestellungen und Kundentransaktionen über B2B Connect und PartsLink24 zu verwalten

Bei der Nutzung von B2B Connect können die Kunden die Produkte, Dienstleistungen und die Gesamtleistung des Partners über den 5*Rater bewerten. Mit seiner Teilnahme und Nutzung des B2B Connect Seller Centers und des WebParts-Händler-Clients nimmt der Partner zur Kenntnis und akzeptiert, dass Kundenfeedback zur Verfügung gestellt wird und dass Mercedes-Benz AG diese Informationen in zusammengefasster Form erhält (ohne Informationen zu bestimmten Transaktionen) und berechtigt ist, diese Informationen für Markt- und Partnerleistungsprüfungen sowie die Steuerung der Gesamtleistung und Zusammenarbeit mit dem Partner zu verwenden. Weitere Einzelheiten zur Verwendung personenbezogener Daten in diesem Zusammenhang sind in **Anhang 1** zu diesen Nutzungsbedingungen aufgeführt.

Auf der Basis der vom Kunden eingegebenen Daten kann der Kunde über das Internet beim Partner Bestellungen vornehmen, wobei der kundenspezifische Preis und die Verfügbarkeit des jeweiligen Mercedes-Benz Originalteils angezeigt werden. Voraussetzung hierfür ist die Registrierung des Kunden für B2B Connect und die Freischaltung des Kunden durch den Partner im WebParts-Händler-Client. Der Kundenauftrag wird über B2B Connect an den Partner übermittelt. Er kann vom Partner über ein Standard-Exportformat ausgelesen und in das Management-System des Partners importiert werden.

Der Partner kann frei wählen, ob und welche der eingegangenen Bestellungen er annehmen möchte. Sofern der Partner und ein Kunde keine anderslautende Vereinbarung getroffen haben, kommt ein Vertrag in dem Moment zustande, in dem der Partner die Bestellung eines Kunden durch Übermittlung einer Bestellungsannahme annimmt. Die Erfüllung der über B2B Connect geschlossenen Verträge liegt in der alleinigen Verantwortung des jeweiligen Partners. Mercedes-Benz AG übernimmt bei Verträgen, die über B2B Connect abgeschlossen werden, keine Gewährleistung für die Erfüllung der zwischen dem Partner und dem Kunden über B2B Connect geschlossenen Verträge. Mercedes-Benz AG ist in keiner Weise verpflichtet, für die Erfüllung der zwischen Partner und Kunden geschlossenen Verträge zu sorgen.

Mercedes-Benz AG ist berechtigt, die über die B2B Connect zur Verfügung gestellten Funktionen zu ändern, wenn eine solche Änderung keine Änderung dieser Nutzungsbedingungen erfordern würde. Mercedes-Benz AG muss den Partner mindestens einen Monat vor einer solchen Änderung in Textform (z. B. per E-Mail) informieren, sofern nicht anders vereinbart.

Sofern nicht anders vereinbart, ist Mercedes-Benz AG berechtigt, diese Nutzungsbedingungen jederzeit einseitig zu ändern, soweit eine solche Änderung für den Partner neutral oder vorteilhaft ist. Ansonsten muss Mercedes-Benz AG den Partner mindestens sechs (6) Wochen vor einer solchen Änderung in Textform informieren. Widerspricht der Partner diesen Änderungen nicht innerhalb von vier (4) Wochen nach Erhalt einer solchen Mitteilung in Textform, werden die vorgeschlagenen Änderungen sechs (6) Wochen nach der Mitteilung für die Vertragspartner verbindlich. Mercedes-Benz AG AG muss den Partner zusammen mit einer solchen Mitteilung über die Rechtsfolgen des Schweigens gegen diese Änderungen informieren. Der Partner hat das Recht, solchen Änderungen zu widersprechen. Widerspricht der Partner, hat Mercedes-Benz

AG das Recht, die Nutzung der von einer solchen Änderung betroffenen Dienste durch den Partner aus wichtigem Grund zu kündigen.

Im Falle der direkten Integration des WebParts-Händler-Clients in das B2B Connect Seller Center durch Mercedes-Benz AG finden die vorliegenden Nutzerbedingungen weiterhin Anwendung, vorbehaltlich ggf. notwendiger Änderungen an diesen Nutzungsbedingungen, die in diesem Zusammenhang entsprechend den vorstehenden Regelungen umgesetzt werden müssen.

§ 3 Nutzung des B2B Connect Seller Centers und des WebParts-Händler-Client

Der Partner erhält über den WebParts-Händler-Client interessierte Kunden, die er für die Online-Bestellung aktivieren kann. Die Aktivierung sollte ohne unangemessene Verzögerung erfolgen.

Es liegt in der Verantwortung des Partners, die Einhaltung der vertraglichen Verkaufsbeschränkungen (Kundendienst- und Teilevertriebsvertrag) sicherzustellen.

Die Stammdaten, z. B. Definition von Rabattsätzen für selbst definierte Kundenrabattklassen, Zuordnung von Mercedes-Benz Originalteilen zu selbst definierten Rabattgruppen oder Aktionen usw. müssen vom Partner in das System eingegeben werden.

Der Partner ist frei in seiner Preisgestaltung, der Gewährung von Rabatten und der Kennzeichnung von Kundenrabatten. Die Preise, Rabatte, Kundenrabatt-Codes oder Kampagnen, die im System gespeichert sind oder von dem Partner eingegeben werden, werden dem Kunden angezeigt, wenn er die Bestellung aufgibt. Es liegt in der Verantwortung des Partners, sicherzustellen, dass die Daten aktuell sind.
Der Partner ist verpflichtet, seine Allgemeinen Geschäftsbedingungen sowie Datenschutzbestimmungen für seine Kunden im WebParts-Händler-Client einzustellen (und die jeweilige Zustimmung im erforderlichen Umfang einzuholen). Aus den Allgemeinen Geschäftsbedingungen des Partners muss hinreichend deutlich hervorgehen, dass der Partner der Verkäufer der Originalteile ist. Aus den Datenschutzbestimmungen muss hinreichend deutlich hervorgehen, dass der Partner für die Daten seiner Kunden im Zusammenhang mit der Durchführung eines Auftrags verantwortlich ist. Darüber hinaus müssen die Datenschutzbestimmungen des Partners die jeweils geltenden datenschutzrechtlichen Bestimmungen (einschließlich etwaiger Informationspflichten), insbesondere die der Datenschutz-Grundverordnung (DSGVO), beachten. Sollte der Partner zu irgendeinem Zeitpunkt während der Laufzeit dieser Nutzungsbedingungen nicht in der Lage sein, die Originalteile in Übereinstimmung mit den geltenden Datenschutzgesetzen anzubieten, muss der Partner Mercedes-Benz AG informieren. Der Partner hat die Möglichkeit, innerhalb einer angemessenen, von Mercedes-Benz AG geforderten Frist einen Vorschlag zur Abhilfe zu machen. Ist eine vom Partner vorgeschlagene Lösung für Mercedes-Benz AG nicht zumutbar, hat Mercedes-Benz AG das Recht, diese Nutzungsbedingungen ganz oder teilweise mit sofortiger Wirkung zu kündigen.

Ziel von B2B Connect ist die Online-Präsentation der Angebote des Partners in Bezug auf Originalteile. Die Kunden dürfen B2B Connect nur zu diesem Zweck nutzen.

Die Nutzung von B2B Connect überträgt keinerlei Rechte an B2B Connect, , den verwendeten URLs oder den begleitenden Dokumentationen (Handbuch, Guided Tour usw.) außer dem Recht zur Nutzung in Übereinstimmung mit diesen Nutzungsbedingungen.

Der Partner verpflichtet sich, dafür Sorge zu tragen, dass die von ihm bei der Nutzung des B2B Connect Seller Centers und des WebParts-Händler-Client, WebParts eingesetzte Hard- und Software einschließlich Arbeitsplatzrechner, Tablets, Router, Datenkommunikationssysteme usw. frei von Viren, Würmern, Trojanischen Pferden usw. ist. Hinsichtlich der vom Partner hochgeladenen Daten stellt der Partner sicher, dass er Inhaber aller Rechte an den hochgeladenen Daten ist und über deren Nutzung frei verfügen kann, einschließlich, dass die hochgeladenen Daten nicht mit Rechten Dritter belastet sind, die einer solchen Nutzung entgegenstehen.

Auf Anfrage des Kunden kann der Partner den Kunden über das B2B Connect Seller Center bei Beschwerden an Mercedes-Benz AG oder anderen Anfragen zu B2B Connect unterstützen. Eine solche Unterstützung ist unentgeltlich (kein Anspruch auf Schadensersatz oder Erstattung von Kosten sowie Auslagen gegenüber Mercedes-Benz AG) und wird ausschließlich in eigener Verantwortung und Beziehung des Partners zum Kunden erfolgen, ohne dass Mercedes-Benz AG eine Verantwortung für die Nutzung des B2B Connect Seller Centers durch den Partner oder zusätzlichen Kunden erbrachten Support übernimmt. Dies gilt auch für die Bereitstellung sonstiger transaktionsbezogener Informationen, die Kunden vom Partner über den WebParts-Händler-Client bereitgestellt werden (z. B. Informationen zur voraussichtlichen Lieferzeit).

§ 4 Datenfluss

Der Kunde gibt seine Daten durch Selbstregistrierung in B2B Connect ein. Diese Daten werden authentifiziert und durch den Anbieter Mercedes-Benz AG gespeichert.
Diese Daten werden dem Partner auch im B2B Connect Seller Center zur Verfügung gestellt.

§ 5 Vertraulichkeit

Die Vertragspartner müssen alle technischen und wirtschaftlichen Informationen, einschließlich der Nutzungsdaten der Kunden, die ihnen während der Laufzeit dieser Nutzungsbedingungen im Zusammenhang mit der Nutzung von B2B Connect direkt oder indirekt zugänglich sind, vertraulich behandeln. Diese Daten dürfen von Mercedes-Benz AG nur dann Dritten zugänglich gemacht werden, wenn dies zur Vertragserfüllung erforderlich oder anderweitig vorgesehen ist und eine entsprechende Vertraulichkeitsvereinbarung mit diesen Dritten besteht. Daten über vom Partner freigeschaltete Kunden oder Kundennutzungsdaten werden von Mercedes-Benz AG nur zur Erfüllung dieser Nutzungsbedingungen verwendet und von MBAG für die Weiterentwicklung der Plattform anonymisiert.

Informationen und Dokumente, die nicht als vertrauliche Informationen eingestuft sind, sind :

- allgemein bekannte Informationen oder Informationen, die ohne Verstoß gegen die in diesen Nutzungsbedingungen enthaltenen Verpflichtungen bekannt werden,
- Informationen, die eine Partei nachweislich als Teil ihrer eigenen Arbeit erstellt oder gewonnen hat, oder
- Informationen, die Mercedes-Benz AG nachweislich rechtmäßig von Dritten erhalten hat.

Eine Partei ist von der Verpflichtung zur vertraulichen Behandlung von Informationen befreit, wenn diese Partei die Informationen aufgrund gesetzlicher Vorschriften oder Anordnungen der zuständigen Behörden offenlegen muss.

§ 6 Datenschutz

Hinsichtlich des Verkaufsprozesses von Originalteilen/Dienstleistungen über B2B Connect beabsichtigen die Vertragspartner, die entsprechenden personenbezogenen Daten zwischen unabhängigen Verantwortlichen auszutauschen, wobei Mercedes-Benz AG für die Verarbeitung der personenbezogenen Daten zum Zwecke des Betriebs von B2B Connect verantwortlich ist. Sofern nicht anders vereinbart, beabsichtigen die Vertragspartner im Allgemeinen nicht, eine gemeinsame Verantwortlichkeit in Bezug auf ihre individuelle Verarbeitung der personenbezogenen Daten des Kunden zu schaffen. Soweit die Beziehung zwischen MBAG (und/oder ihren verbundenen Unternehmen) und dem Partner als gemeinsame Verantwortlichkeit gemäß Art. 26 der Datenschutz-Grundverordnung (DSGVO) gilt oder qualifiziert wird, werden die Vertragspartner in Zukunft entsprechende Vereinbarungen über die gemeinsame Verantwortlichkeit mit dem/den jeweiligen gemeinsamen Verantwortlichen abschließen, in denen die jeweiligen Verantwortlichkeiten der gemeinsam Verantwortlichen gemäß Art. 26 DSGVO festgelegt werden.

Ungeachtet des Vorstehenden verarbeitet Mercedes-Benz AG personenbezogene Daten des Partners und der Kunden des Partners (i) im Namen des Partners als Auftragsverarbeiter und (ii) bei der Verwendung personenbezogener Daten im B2BConnect 5*Rater für Support über das B2B Connect Seller Center oder für Geschäftsanalysen und Marketingkampagnendienste als Verantwortlicher. Die zwischen den Vertragspartnern vereinbarten Datenschutzbestimmungen sind in **Anhang 1** zu diesen Nutzungsbedingungen aufgeführt.

§ 7 Datenqualität, Pflichten des Partners

Der Partner ist dafür verantwortlich, die für das Anbieten/Anzeigen der Originalteile über den WebParts-Händler-Client notwendigen Informationen (Preise, Rabatte, Verfügbarkeit, Lieferzeiten usw.) aktuell zu halten.

Der Partner überprüft regelmäßig online oder nach elektronischer Benachrichtigung, ob eine Bestellung von Originalteilen durch den Kunden erfolgt ist. Der Partner exportiert diese Bestellungen in das Händlersystem und bearbeitet sie weiter. Der Partner wird die Bestellungen innerhalb einer angemessenen Frist bearbeiten und den Kunden über den Stand der Bestellung informieren. Eine Auftragsbestätigung an den Kunden, ob die vom Kunden gewünschten Liefertermine eingehalten werden können, hat auf dem üblichen Weg zu erfolgen.

Mercedes-Benz AG stellt ein geeignetes Zugangsschutzsystem zur Verfügung und erteilt dem Partner auf Wunsch eine Zugangsberechtigung. Der Partner verpflichtet sich, die ordnungsgemäße Nutzung des Systems durch seine Mitarbeiter zu gewährleisten, einschließlich der Verwendung geeigneter Anwendungen beim Zugriff auf das System. Der Partner verpflichtet sich, die ihm erteilte Zugangsberechtigung nicht an Unbefugte weiterzugeben.
Der Partner verpflichtet sich, auf eingehende Registrierungsannahmeanfragen von Kunden innerhalb einer angemessenen Zeit zu reagieren und in Abstimmung mit Mercedes-Benz AG 1st und 2nd Level Support für den WebParts-Händler-Client zu leisten. Mercedes-Benz AG schließt jegliche Haftung für den Missbrauch von Benutzer-ID und Passwort in der Organisationseinheit des Partners und seiner Kunden aus.

Mercedes-Benz AG behält sich das Recht vor, den betreffenden Nutzer bei Anzeichen einer missbräuchlichen Nutzung zu sperren. Der Partner wird hierüber direkt informiert.

B2B Connect ist eine weltweit verfügbare technische Lösung. Der Partner ist für die regelmäßige Überprüfung der in seinem Land geltenden rechtlichen Rahmenbedingungen für den Verkauf und den Verkaufsprozess von Originalteilen in B2B Connect verantwortlich, während Mercedes-Benz AG für die regelmäßige Überprüfung der geltenden rechtlichen Rahmenbedingungen für den Betrieb seiner Online-Teile von B2B Connect verantwortlich bleibt.

Der Partner muss insbesondere sicherstellen, dass sämtliche Anforderungen (einschließlich aller erforderlichen Einwilligungen und Informationen) in Bezug auf Kunden erfüllt werden, um die von diesen Nutzungsbedingungen geregelten Services bereitstellen zu können.

In jedem Fall gelten die als **Anhang 2** bereitgestellten Plattformregeln von Mercedes-Benz zusammen mit den vorliegenden Nutzungsbedingungen.

§ 8 Verfügbarkeit

Nach dem derzeitigen Stand der Technik kann die Bereitstellung und Nutzung von B2B Connect auch gewissen Einschränkungen und Ungenauigkeiten unterliegen, die außerhalb des Einflussbereichs von Mercedes-Benz AG liegen. Dies gilt insbesondere für die Verfügbarkeit des Internetzugangs. Störungen können auch durch höhere Gewalt, einschließlich Streiks, Aussperrungen oder behördliche Anordnungen, oder durch technische oder sonstige Maßnahmen (z. B. Reparaturen, Wartungen, Software-Updates und -Erweiterungen) verursacht werden, die auf Systemen von Mercedes-Benz AG oder von Dienstleistern durchgeführt werden müssen, um die ordnungsgemäße Bereitstellung oder Verbesserung von B2B Connect zu gewährleisten.

§ 9 Haftung, Freistellung

Mercedes-Benz AG und Partner haften für sich und ihre Erfüllungsgehilfen bei Vorsatz und grober Fahrlässigkeit sowie bei leichter Fahrlässigkeit im Falle der Verletzung von Leben und Körper.

Ferner haften Mercedes-Benz AG und Partner für leichte Fahrlässigkeit wie folgt: Eine Haftung besteht nur bei der Verletzung wesentlicher Vertragspflichten; "wesentliche Vertragspflichten" sind solche, deren Erfüllung für die ordnungsgemäße Durchführung des Vertrages von wesentlicher Bedeutung ist (Kardinalpflichten). Diese Haftung ist auf den typischen, bei Vertragsschluss vorhersehbaren, unmittelbaren Schaden begrenzt. Soweit der Schaden durch eine vom Partner oder Mercedes-Benz AG für den betreffenden Schaden abgeschlossene Versicherung (ausgenommen Kaskoversicherung) gedeckt ist, haften Mercedes-Benz AG oder der Partner nur für etwaige damit verbundene Nachteile des Partners oder von Mercedes-Benz AG, z. B. höhere Versicherungsprämien oder Zinsnachteile, bis zur Abwicklung der Versicherung.

Der Partner ist verpflichtet, Mercedes-Benz AG von allen Schäden, Verlusten, Verbindlichkeiten, Ansprüchen (einschließlich Ansprüchen Dritter) und Kosten (einschließlich der dazugehörigen Anwaltsgebühren und -kosten) freizustellen, die sich aus einer schuldhaften Verletzung der vorliegenden Bedingungen und der hierin geregelten Transaktionen (einschließlich aber nicht beschränkt auf die Nutzung des Seller Centers durch den Partner) ergeben.

§ 10 Dauer und Beendigung der Nutzungsbedingungen

Diese Nutzungsbedingungen ersetzen die vorherigen Nutzungsbedingungen in Bezug auf denselben Gegenstand mit Wirkung vom 01 Januar 2025 und treten mit ihrer Annahme in Kraft.

Beide Vertragspartner können diese Nutzungsbedingungen mit einer Frist von drei Monaten zum Monatsende schriftlich (für alle Kündigungen nach diesem § 10 genügt die Textform) kündigen. In

jedem Fall enden diese Nutzungsbedingungen mit der Beendigung des Kundendienst- und Teilevertriebsvertrags zwischen den Vertragspartnern.

Nach Beendigung der Nutzungsbedingungen bleiben die in § 4, 5 und 6 genannten Bestimmungen zum Datenschutz und zur Vertraulichkeit weiter bestehen.

Bei schwerwiegenden Verstößen gegen diese Nutzungsbedingungen, wie z. B. bei der Übermittlung von Daten, die einen Verstoß gegen die Geheimhaltungspflicht nach § 5 darstellen, kann jede Partei diese Nutzungsbedingungen fristlos kündigen. Im Falle einer Kündigung aufgrund einer schwerwiegenden Vertragsverletzung durch eine Partei behält sich die andere Partei das Recht vor, weitere Schäden geltend zu machen.

§ 11 Steuern

Falls Mercedes-Benz AG Steuern und Zölle zu entrichten hat, die auf den Verkauf von Produkten, die der Partner im WebParts-Händler-Client und B2B Connect Seller Center eingestellt hat, oder auf Dienstleistungen, die der Partner in B2B Connect eingestellt und dem Kunden zur Verfügung gestellt hat, wie z. B. Steuern auf digitale Dienstleistungen, entfallen, wird der Partner alle Mercedes-Benz AG durch solche Steuern und Zölle entstehenden Kosten übernehmen. Entsprechendes gilt für geschuldete und vom Partner nicht abgeführte Mehrwertsteuer, für die Mercedes-Benz AG haftbar gemacht wurde.

§ 12 Gerichtsstand

Diese Nutzungsbedingungen unterliegen dem Recht der Bundesrepublik Deutschland]. Ausschließlicher Gerichtsstand für Streitigkeiten, die sich aus diesen Bedingungen ergeben, ist Stuttgart

Anhänge zu diesen Nutzungsbedingungen

Anhang 1 – Datenschutzvereinbarung
Anhang 2 – Plattformregeln

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Anhang 1:

Datenschutzvereinbarung

B2B Connect-Plattform und zugehörige Dienste

zwischen

Mercedes-Benz AG

("**MBAG**")

und

Autorisierter Servicepartner

("ASP")

(jeweils ein "**Vertragspartner**", und zusammen die "**Vertragspartner**").

HINTERGRUND

(A) Mercedes-Benz AG ist ein Unternehmen der Mercedes-Benz-Group AG und unterstützt das Geschäft in Bezug auf ihre Händler ("Händler", einschließlich ISP-Kunden ("ISP") und autorisierte Servicepartner) in Deutschland, Europa (EU) und dem Rest der Welt ("RoW") durch das Angebot bestimmter Aftersales- und marketingbezogener Dienstleistungen ("Dienstleistungen", wie unten definiert).

(B) Das Angebot und die Erbringung der Dienste beinhaltet die Übermittlung und Verarbeitung personenbezogener Daten an und durch Mercedes-Benz AG zur Erbringung der Dienste für ASPs.

(C) Die europäischen und lokalen Datenschutzgesetze sehen bestimmte Anforderungen vor, u. a. für die Übermittlung und Verarbeitung personenbezogener Daten innerhalb von Unternehmensgruppen oder Vertriebs- oder Kundendienstnetzen.

(D) ***Diese*** Vereinbarung soll angemessene Garantien und einen angemessenen Schutz bei der nationalen, grenzüberschreitenden, EU-weiten und weltweiten Übermittlung und Verarbeitung personenbezogener Daten gemäß den nachstehend definierten anwendbaren Datenschutzgesetzen bieten.

(E) ***Daher*** schließen die Parteien die folgende Vereinbarung (nachstehend "Vereinbarung" genannt).

1. BEGRIFFSBESTIMMUNGEN

1.1 In dieser Vereinbarung haben die folgenden Begriffe die folgende Bedeutung:

(a) Die Begriffe "personenbezogene Daten", "für die Verarbeitung Verantwortlicher", "Auftragsverarbeiter", "Verarbeitung", "betroffene Person", "technische und organisatorische Maßnahmen" und "Aufsichtsbehörde/Behörde" sind im Einklang mit der Datenschutz-Grundverordnung (DSGVO) oder der entsprechenden Terminologie der geltenden Datenschutzgesetze auszulegen. Unterauftragsverarbeiter hat die gleiche Bedeutung wie "ein anderer Auftragsverarbeiter" in der DSGVO oder die entsprechende Terminologie in den geltenden Datenschutzgesetzen.

(b) "Vereinbarung" bezeichnet diese Datenschutzvereinbarung.

(c) "Anwendbare Datenschutzgesetze" sind die DSGVO, alle lokalen Datenschutzgesetze, die in einem Mitgliedstaat gelten, oder alle anderen anwendbaren Datenschutzgesetze, die für jede der Parteien – gemeinsam oder getrennt – bei der Erbringung oder Nutzung der Dienste gelten. Die Tatsache, dass eine Partei die vorliegende Vereinbarung entsprechend unterzeichnet hat, bedeutet nicht, dass auf eine Partei anwendbare Datenschutzgesetze automatisch auf die andere(n) Partei(en) Anwendung finden. Abgesehen von den Bestimmungen dieser Vereinbarung richtet sich die Anwendbarkeit der anwendbaren Datenschutzgesetze auf die einzelnen Parteien nach den jeweiligen Gesetzen . Vorbehaltlich weiterer Bestimmungen und Pflichten der Parteien, die in dieser Vereinbarung festgelegt werden, muss sich jede Partei dementsprechend an die anwendbaren Datenschutzgesetze halten, sofern und soweit diese nur auf sie Anwendung finden. Zur Klarstellung: Wenn beispielsweise auf gesetzliche Rechte von betroffenen Personen gemäß Artikeln 12–22 DSGVO oder gesetzliche Anforderungen für die Auftragsdatenerarbeitung gemäß Artikel 28 DSGVO Bezug genommen wird, gelten solche Rechte oder Anforderungen nur für Verantwortliche, die in den Geltungsbereich der DSGVO fallen.

(d) "Land mit angemessenem Datenschutzniveau" bezeichnet jedes Land außerhalb des EWR, das von der Europäischen Kommission aufgrund seiner innerstaatlichen Rechtsvorschriften oder der von ihm eingegangenen internationalen Verpflichtungen als Land anerkannt wird, das ein angemessenes Datenschutzniveau bietet.

(e) "Datenverarbeitung im Auftrag eines Verantwortlichen" bezeichnet die Verarbeitung personenbezogener Daten, die im Auftrag eines für die Verarbeitung Verantwortlichen durchzuführen ist, und ist im Sinne des Artikels 28 der DSGVO auszulegen.

(f) "MBAG" bedeutet Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Deutschland.

(g) "Klauseln" bezeichnet zusammenfassend die Klauseln über die Datenverarbeitung im Auftrag eines Verantwortlichen und die Klauseln über die Verarbeitung zwischen Verantwortlichen.

(h) "Klauseln über die Datenverarbeitung im Auftrag eines Verantwortlichen" sind die in Teil B aufgeführten Bestimmungen.

(i) "Klauseln zwischen gemeinsam Verantwortlichen" sind die Bestimmungen in Teil A. Die Klauseln zwischen den gemeinsam Verantwortlichen regeln die Übermittlung und Verwendung personenbezogener Daten zwischen Mercedes-Benz AG und dem ASP, wobei die Parteien jeweils als gemeinsam für die Verarbeitung Verantwortliche handeln, sofern dies nach den geltenden Datenschutzgesetzen für jeden von ihnen vorgesehen ist.

(j) "DSGVO" bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

(k) "Gemeinsame Verantwortlichkeit" bedeutet die Verarbeitung personenbezogener Daten, deren Zweck von zwei oder mehreren Verantwortlichen gemeinsam festgelegt wird, und ist gemäß Artikel 26 der DSGVO auszulegen.

(l) "Mitgliedstaat" ist ein Land, das Mitglied der EU ist.

(m) "Dienstleistungen" sind die in den entsprechenden separaten Verträgen und Teilen dieser Vereinbarung näher beschriebenen Aftersales-bezogenen Dienstleistungen.

1.2 In dieser Vereinbarung gilt Folgendes:

(a) Verweise auf eine gesetzliche Bestimmung schließen alle nachgeordneten Rechtsvorschriften ein, die von Zeit zu Zeit auf der Grundlage dieser Bestimmung erlassen werden;

(b) Verweise auf diese Vereinbarung schließen die Anhänge und Anlagen ein;

(c) Überschriften werden bei der Auslegung dieser Vereinbarung nicht berücksichtigt; und

(d) Sollte es innerhalb dieser Vereinbarung zu Konflikten oder Unstimmigkeiten kommen, so werden diese durch die vorrangig geltenden Klauseln gelöst.

2. GELTUNGSBEREICH

2.1 Die Klauseln gelten zwischen den Parteien in ihrer Rolle als für die Verarbeitung Verantwortliche (oder gemeinsam für die Verarbeitung Verantwortliche) oder als Auftragsverarbeiter in Bezug auf die betreffenden personenbezogenen Daten, die gemäß den Anhängen zu den Teilen A und B verarbeitet werden.

2.2 Da die Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten ein angemessenes Schutzniveau im Hinblick auf den Schutz der Privatsphäre und der Grundrechte und -freiheiten der betroffenen Personen gewährleisten wollen, gelten die in Teil A dargelegten Grundsätze für die dort beschriebene Verarbeitung zwischen Verantwortlichen, unabhängig davon, ob es sich um eine Verarbeitung im Rahmen einer gemeinsamen Kontrollinstanz handelt oder nicht.

2.3 Jede Vertragspartei verpflichtet in ihrer Eigenschaft als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter etwaige Unterauftragsverarbeiter dazu, mindestens ein ähnliches Schutzniveau zu bieten, und stellt darüber hinaus sicher, dass der Unterauftragsverarbeiter die Sicherheits- und Datenschutzrichtlinien und -anforderungen von Mercedes-Benz AG erfüllt, bevor er eine entsprechende Vereinbarung mit einem Unterauftragsverarbeiter schließt.

3. ÄNDERUNGEN

Die Parteien können diese Vereinbarung gemäß dem in der zugrunde liegenden Vereinbarung (Terms of Use_ASP_B2B Connect) vereinbarten Verfahren aktualisieren oder ergänzen.

4. LAUFZEIT UND KÜNDIGUNG

4.1 Diese Vereinbarung tritt mit der Unterzeichnung durch beide Parteien in Kraft, indem diese Bedingungen elektronisch akzeptiert werden (als Teil der jeweiligen Geschäftsbedingungen). Jede Vertragspartei ist von dem Zeitpunkt an, an dem sie die Vereinbarung ordnungsgemäß unterzeichnet hat, an die darin enthaltenen Bestimmungen und Bedingungen gebunden.

4.2 Diese Vereinbarung gilt so lange, bis das Vertragsverhältnis (zu dem diese Vereinbarung gehört) zwischen den Parteien beendet wird oder die Dienstleistungen nicht mehr erbracht werden, je nachdem, welches Ereignis weiter in der Zukunft liegt, wobei die Verpflichtungen der Parteien aus dieser Vereinbarung so lange bestehen, wie personenbezogene Daten einer Partei von der anderen Partei verarbeitet werden.

5. MITTEILUNGEN

Jede Mitteilung im Rahmen dieser Vereinbarung ("**Mitteilung**") muss in Textform erfolgen.

6. ABTRETUNG

Der ASP darf ohne vorherige schriftliche Zustimmung von Mercedes-Benz AG keine Rechte oder Pflichten aus dieser Vereinbarung abtreten oder übertragen.

7. Haftung

Die Parteien haften einander für alle Ansprüche Dritter oder sonstige Verluste oder Schäden, für die sie verantwortlich sind (insbesondere für Schäden, die in ihrem jeweiligen Einflussbereich entstanden sind) und die sich aus der Verletzung ihrer Verpflichtungen aus dieser Vereinbarung und/oder aus sonstigen Verstößen gegen geltende Datenschutzgesetze ergeben, es sei denn, die andere Partei wurde nicht auf solche Verpflichtungen hingewiesen. Ist eine der Vertragsparteien nach den geltenden Datenschutzgesetzen verpflichtet, den einer betroffenen Person entstandenen Schaden in vollem Umfang zu ersetzen, und ist sie dieser Verpflichtung nachgekommen, so ist sie berechtigt, von der anderen Vertragspartei

den Teil des Schadensersatzes zu verlangen, der dem Anteil der anderen Vertragspartei an der Verantwortung für den Schaden entspricht.

8. SALVATORISCHE KLAUSEL

8.1 Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtswidrig, ungültig oder nicht durchsetzbar sein, so wird die Rechtmäßigkeit, Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen dieser Vereinbarung nicht berührt.

8.2 Die Parteien vereinbaren, die unwirksame Bestimmung durch eine solche zu ergänzen, die in ihrer Wirkung dem von den Parteien verfolgten wirtschaftlichen Ziel am nächsten kommt. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich diese Vereinbarung als lückenhaft erweist.

9. ANWENDBARES RECHT UND GERICHTSSTAND

Erfüllungsort ist die Bundesrepublik Deutschland, Gerichtsstand ist das zuständige Gericht in Deutschland, Baden-Württemberg, Stuttgart. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Die Parteien vereinbaren, die Anwendung des einheitlichen Kaufrechts der Vereinten Nationen (UN), das auf dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980 beruht, auszuschließen.

10. VERHÄLTNIS ZU GESONDERTEN VEREINBARUNGEN

10.1 Diese Vereinbarung ersetzt alle bisher zwischen den Parteien bestehenden Datenschutzregelungen in Bezug auf die hier ausdrücklich geregelten Datenverarbeitungstätigkeiten.

10.2 Alle hier nicht ausdrücklich geregelten Fragen, einschließlich der Haftung der Parteien bei der Erbringung oder Nutzung der jeweiligen Dienste oder der Übermittlung der jeweiligen Daten zu den angegebenen Zwecken, richten sich nach den Bestimmungen etwaiger weiterer zwischen den Parteien bestehender Vereinbarungen (die sich aus dem in Abschnitt 4.2 dargelegten Vertragsverhältnis ergeben).

10.3 Im Falle von Widersprüchen zwischen den Bestimmungen dieser Vereinbarung und den in Abschnitt 10.2 genannten anderen Vereinbarungen sind die Bestimmungen dieser Vereinbarung maßgebend.

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Teil A

KLAUSELN ZWISCHEN GEMEINSAM VERANTWORTLICHEN

Präambel

Im Rahmen ihrer geschäftlichen Zusammenarbeit im Hinblick auf B2B Connect beabsichtigen die Parteien, für bestimmte geschäftliche Zwecke personenbezogene Daten weiterzugeben und sie als für die Daten Verantwortliche im Sinne des Datenschutzrechts zu verarbeiten (im Folgenden "Zusammenarbeit" genannt).

In diesen Klauseln (im Folgenden "Vereinbarung" genannt) legen die Parteien ihre Rechte und Pflichten bezüglich der Verarbeitung personenbezogener Daten im Rahmen der Zusammenarbeit sowie die jeweiligen Verantwortlichkeiten hinsichtlich der Einhaltung einschlägiger Datenschutzpflichten fest.

Vor diesem Hintergrund treffen die Parteien folgende Vereinbarung:

1. Gegenstand der Vereinbarung

Die vorliegende Vereinbarung regelt die Rechte und Pflichten der Parteien (im Folgenden auch "Verantwortliche") im Rahmen der Verarbeitung personenbezogener Daten als gemeinsam Verantwortliche.

2. Umfang der Verarbeitung unter gemeinsamer Verantwortung

2.1 Während der Zusammenarbeit verarbeiten die Parteien personenbezogene Daten als gemeinsam Verantwortliche im Sinne von Artikel 26 DSGVO. Die Bestimmungen der vorliegenden Vereinbarung gelten für sämtliche Verarbeitungstätigkeiten, die unter gemeinsamer Verantwortung ausgeführt werden, wobei die Mitarbeiter der Verantwortlichen oder der von diesen beauftragten Auftragsverarbeiter personenbezogene Daten im Auftrag der Verantwortlichen verarbeiten. Der Umfang der Verarbeitung als gemeinsam Verantwortliche, einschließlich der jeweiligen Rollen, Zuständigkeiten und Kompetenzen, sowie weitere Einzelheiten der Verarbeitung sind in Anlage 1 dargelegt.

2.2 Die Informationen in Anlage 1 werden durch die Prozess- und Tätigkeitsbeschreibungen in den parallel von den Parteien geschlossenen Verträgen (z. B. Serviceverträge), einschließlich der parallel bereitgestellten Informationstexte, auf die Bezug genommen wird, ergänzt.

3. Aufgaben der Verantwortlichen

3.1 Die Verantwortlichen führen die Verarbeitung personenbezogener Daten in Übereinstimmung mit den einschlägigen Bestimmungen der anwendbaren Datenschutzgesetze durch und sind entsprechend der DSGVO gemeinsam für die Verarbeitungstätigkeiten wie von dieser Vereinbarung abgedeckt und vorgegeben verantwortlich. So müssen sie insbesondere sicherstellen, dass nur die personenbezogenen Daten erhoben werden, die für die in Anlage 1 beschriebenen Verarbeitungstätigkeiten und -zwecke benötigt werden. Zudem müssen die Verantwortlichen den Grundsatz der Datenminimierung beachten (vgl. Artikel 5 Absatz 1 Buchstabe c DSGVO).

3.2 Intern ist jede Partei für die Rechtmäßigkeit der Erhebung und Verarbeitung personenbezogener Daten im Rahmen der ihr nachstehend und in Anlage 1 zugewiesenen Aufgaben und Zuständigkeiten verantwortlich.

3.3 Die Verantwortlichen stellen sicher, dass sämtliche Personen, die an der im Rahmen der Zusammenarbeit durchgeführten Verarbeitung personenbezogener Daten beteiligt sind, vor ihrem Zugriff auf entsprechende Daten zur Vertraulichkeit und Wahrung des Datengeheimnisses verpflichtet sind oder werden und während ihrer Tätigkeiten sowie über die Beendigung ihrer Tätigkeiten hinaus daran gebunden sind. Sie müssen dafür Sorge tragen, dass die betreffenden Personen in den für sie geltenden Datenschutzbestimmungen unterwiesen werden.

3.4 Die Verantwortlichen speichern personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format. Personenbezogene Daten müssen korrekt sein und, soweit erforderlich, auf dem neuesten Stand gehalten werden. Die Verantwortlichen ergreifen sämtliche Maßnahmen, um dies zu gewährleisten.

3.5 Die Verantwortlichen informieren sich gegenseitig unverzüglich und vollumfänglich, wenn sie bei der Überprüfung von Verarbeitungstätigkeiten Fehler oder Unregelmäßigkeiten im Hinblick auf die Datenschutzbestimmungen feststellen.

3.6 Dokumentation, die als Nachweis der ordnungsgemäßen Verarbeitung dient (vgl. Artikel 5 Absatz 2 DSGVO), ist von jeder Partei im Einklang mit ihren rechtlichen Befugnissen und Pflichten über die Beendigung der Vereinbarung hinaus aufzubewahren.

4. Technische und organisatorische Maßnahmen

4.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen die Verantwortlichen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, unter anderem auch gegebenenfalls in Bezug auf Folgendes:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste kontinuierlich zu gewährleisten;
- die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls schnell wiederherzustellen;
- ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung; und
- ein Verfahren zur ordnungsgemäßen Einhaltung der Datenschutzgrundsätze durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. Artikel 25 DSGVO).

Die Verantwortlichen können getrennt voneinander zusätzliche Anforderungen festlegen.

4.2 Die Verantwortlichen ergreifen alle technischen und organisatorischen Maßnahmen, die erforderlich sind, um sicherzustellen, dass die Rechte der betroffenen Personen, insbesondere gemäß Artikeln 12–22 DSGVO, jederzeit entsprechend den rechtlichen Anforderungen ausgeübt werden können. Falls notwendig verständigen sich die Verantwortlichen auf die genaue Gestaltung der Maßnahmen und beschließen gemeinsam deren Umsetzung.

4.3 Die Implementierung, die Voreinstellungen und der Betrieb der Systeme müssen die Anforderungen der anwendbaren Datenschutzgesetze erfüllen und insbesondere die Grundsätze "Privacy by design" und "Privacy by default" einhalten sowie unter Anwendung angemessener, dem Stand der Technik entsprechender technischer und organisatorischer Maßnahmen erfolgen.

5. Verantwortung für die Beachtung der Datenschutzgesetze und Rechte betroffener Personen

5.1 Betroffene Personen können gegenüber Verantwortlichen die ihnen gemäß Artikeln 12–22 DSGVO gewährten Rechte geltend machen, wobei die Verantwortlichen für die Erfüllung der jeweiligen Rechte im Außenverhältnis verantwortlich bleiben.

5.2 Sofern in Anlage 1 oder in einem anderen Zusammenhang nichts anderes vorgesehen ist, bleibt der Verantwortliche, der die personenbezogenen Daten der betroffenen Person vor deren Übermittlung an den anderen Verantwortlichen zur Weiterverarbeitung ursprünglich erhoben hat oder der in einem direkten Vertragsverhältnis mit der betroffenen Person stand oder steht, zentrale Anlaufstelle für die betroffenen Personen und unterstützt den der DSGVO unterliegenden Verantwortlichen bei seinen Pflichten im Hinblick auf die Erfüllung der Rechte von betroffenen Personen gemäß der Artikel 12–22 DSGVO im Innenverhältnis. Diese Unterstützung erfolgt auf eine Weise, die es dem anderen Verantwortlichen gestattet, den genannten Rechten vollumfänglich zu entsprechen.

5.3 Die Verantwortlichen unterstützen einander in angemessenem Umfang bei der Erfüllung der Rechte von betroffenen Personen, informieren sich gegenseitig über entsprechende Anträge und stellen sich rechtzeitig sämtliche erforderlichen Informationen bereit. Sofern personenbezogene Daten zu löschen sind, setzen sich die Parteien rechtzeitig im Voraus darüber in Kenntnis. Die jeweils andere Partei kann der Löschung aus triftigem Grund widersprechen, beispielsweise, wenn sie zur Aufbewahrung der Daten rechtlich verpflichtet.

5.4 Betroffene Personen werden gemäß Artikeln 13 und 14 DSGVO über die Verarbeitung in Kenntnis gesetzt. Die Verantwortlichen unterstützen sich gegenseitig bei der Erfüllung ihrer Informationspflichten und stellen einander die erforderlichen Informationen über die relevanten Datenverarbeitungstätigkeiten zur Verfügung.

5.2 Sofern in Anlage 1 oder in einem anderen Zusammenhang nichts anderes vorgesehen ist, bleibt der Verantwortliche, der die personenbezogenen Daten der betroffenen Person vor deren Übermittlung an den anderen Verantwortlichen zur Weiterverarbeitung ursprünglich erhoben hat oder der in einem direkten Vertragsverhältnis mit der betroffenen Person stand oder steht, dafür verantwortlich, die betroffenen Personen über die wesentlichen Inhalte dieser Regelungen zu informieren. Dazu kann der Verantwortliche den betroffenen Personen auf Anfrage die Bestimmungen dieses Abschnitts 6 vorlegen.

5.6 Jeder Verantwortliche unterliegt den Melde- und Mitteilungspflichten infolge einer möglichen Verletzung des Schutzes personenbezogener Daten gegenüber der Aufsichtsbehörde und den von der Verletzung betroffenen Personen in seinem jeweiligen Zuständigkeitsbereich (vgl. Artikel 33, 34 DSGVO). Im Falle eines zu meldenden Vorfalls im Zusammenhang mit den von dieser Vereinbarung abgedeckten Verarbeitungstätigkeiten informieren die Verantwortlichen einander unverzüglich, bevor sie den Vorfall an die Aufsichtsbehörde melden oder die betroffenen Personen informieren. Die Verantwortlichen unterstützen einander bestmöglich bei der Klärung der Fakten und Ergreifung angemessener Maßnahmen zum Schutz der betroffenen Personen. Die Entscheidung über die Notwendigkeit, den Inhalt und den Umfang der zu ergreifenden Maßnahmen trifft jeweils der für die Verarbeitung Verantwortliche, der zur Mitteilung verpflichtet ist.

5.7 Die Parteien unterstützen sich nach Bedarf und auf Verlangen bei der Vorbereitung von Datenschutz-Folgenabschätzungen (vgl. Artikel 35 DSGVO) oder der Konsultation der Aufsichtsbehörde (vgl. Artikel 36 DSGVO). Die Parteien stellen einander rechtzeitig die dazu benötigten Informationen aus ihren jeweiligen Zuständigkeitsbereichen zur Verfügung.

5.8 Jeder für die Verarbeitung Verantwortliche führt ein Verzeichnis der Verarbeitungstätigkeiten unter seiner Verantwortung. Die Verantwortlichen teilen sich gegenseitig die Informationen mit, die für die Führung eines entsprechenden Verzeichnisses der Verarbeitungstätigkeiten erforderlich sind.

5.9 Die Dokumente, die als Nachweis für die ordnungsgemäße Datenverarbeitung dienen (siehe Abschnitt 5.6), werden von jeder Partei über das Ende des Vertragsverhältnisses hinaus aufbewahrt. Die Verantwortlichen stellen sicher, dass sie allen bestehenden rechtlichen Verpflichtungen im Hinblick auf die Aufbewahrung der betreffenden personenbezogenen Daten nachkommen.

5.10 Sofern nichts anderes vereinbart wurde, trägt jeder Verantwortliche seine eigenen Kosten, die ggf. bei der Erfüllung seiner Pflichten aus dieser Vereinbarung entstehen, wobei er nicht berechtigt ist, von dem anderen Verantwortlichen für die Erfüllung der Pflichten eine Vergütung zu verlangen.

6. Verarbeiter

6.1 Jeder Verantwortliche ist berechtigt, Auftragsverarbeiter einzusetzen.

6.2 Sofern ein Verantwortlicher für die Verarbeitungstätigkeiten unter dieser Vereinbarung einen Auftragsverarbeiter einsetzt, erfolgt dies ausschließlich, soweit die Anforderungen der anwendbaren Datenschutzgesetze erfüllt werden.

6.3 Die Verantwortlichen legen einander auf Verlangen eine Liste der Auftragsverarbeiter vor, die an den Datenverarbeitungstätigkeiten gemäß dieser Vereinbarung beteiligt sind. Verantwortliche informieren die jeweils anderen Verantwortlichen auf Verlangen über geplante Änderungen zum Zwecke der Ergänzung oder Ersetzung von Auftragsverarbeitern.

6.4 Dies gilt nicht in Fällen, in denen die Verantwortlichen Dritte mit Nebenleistungen beauftragen. Solche Leistungen umfassen unter anderem Post-, Telekommunikations-, Liefer- und Empfangsdienste sowie Facility-Management-Leistungen. Die Verantwortlichen sind weiterhin verpflichtet, mit den betreffenden Dienstleistern entsprechend den geltenden gesetzlichen Anforderungen angemessene vertragliche Vereinbarungen und Verpflichtungen anzuwenden

sowie für geeignete Kontrollmaßnahmen in Bezug auf die Sicherheit personenbezogener Daten zu sorgen.

7. Verarbeitung innerhalb und außerhalb des Europäischen Wirtschaftsraums

Die Verarbeitung erfolgt in der Regel in einem Mitgliedstaat der Europäischen Union, in einem Land des Europäischen Wirtschaftsraums oder in einem Land mit angemessenem Schutzniveau. Verarbeitungstätigkeiten in anderen Ländern außerhalb des Europäischen Wirtschaftsraums sind zulässig, solange die anwendbaren Bestimmungen hinsichtlich der internationalen Übermittlung personenbezogener Daten eingehalten werden.

8. Haftung

8.1 Die Verantwortlichen haften gegenüber betroffenen Personen gemäß den gesetzlichen Bestimmungen.

8.2 Die Verantwortlichen haften im Innenverhältnis insoweit, dass jeder von ihnen einen Teil der Verantwortung für den Haftungsgrund trägt. Dies gilt auch im Hinblick auf Bußgelder, die für einen Verantwortlichen aufgrund einer Verletzung von Datenschutzbestimmungen verhängt werden, vorausgesetzt dass der Verantwortliche, gegen den das jeweilige Bußgeld erhoben wurde, zunächst alle rechtlichen Mittel gegen die offizielle Entscheidung ausgeschöpft hat. Unterliegt ein Verantwortlicher dann weiterhin einem Bußgeld, das nicht seinem internen Anteil an der Verantwortung für die Verletzung entspricht, ist der jeweils andere Verantwortliche verpflichtet, den von dem Bußgeld betroffenen Verantwortlichen in der Höhe zu entschädigen, wie es seiner Verantwortung für die dem Bußgeld zugrunde liegenden Verletzung entspricht.

8.3 Jedwede Haftungsbeschränkung, die in Zusatzverträgen für die relevanten Leistungen vereinbart wurde, findet entsprechend Anwendung.

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Anlage 1: Rollen, Aufgaben und Umfang der Zusammenarbeit

1. Business Analytics-bezogene Verarbeitungstätigkeiten

Verfahren	Zweck/ Umfang	Rollen und Aufgaben	Datenkategorien und betroffene Personen
Ticket-Support für ISPs im Seller Center	Möglichkeit für ASPs, ISPs bei Tickets im Seller Center und Anfragen zur Kontoeröffnung zu unterstützen.	Mercedes-Benz AG: Controller Ermöglicht dem ASP, ISPs bei Tickets im Seller Center zu unterstützen, und stellt dem ASP nach Mitteilung an den ISP Ticket- und Anfrageinformationen zur Verfügung; Verantwortung für die technische Verarbeitung von Ticketinformationen ASP: Controller Unterstützt ISP bei Tickets/Anfragen in Zusammenarbeit mit dem ISP; Verantwortung für den ordnungsgemäßen Umgang mit den bereitgestellten Informationen und die richtige Verarbeitung	ISP-Daten: ISP-Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon, Ticket- oder Anfragedetails (Datum, Gegenstand) ASP-Daten: Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon
Business Analytics	Die durch den Betrieb der B2B Connect-Plattform gewonnenen Umsatzdaten werden zur Analyse des Geschäftsbetriebs und zur Erstellung aggregierter Berichte an MBAG und den ASP verwendet. Berichte werden in der Regel durch automatische Berechnungen (anwendungsbezogen) erstellt. In Ausnahmefällen werden die Daten mit Daten aus anderen Quellen (z. B. einer anderen Datenbank einer anderen MBAG-Abteilung) zusammengeführt, um weitere Analysen durchzuführen. Die MBAG und ihre Mitarbeiter arbeiten streng nach dem Erforderlichkeitsprinzip.	MBAG: Controller Betreibt Geschäftslogik und hostet Datenbank mit Geschäftsdaten, erstellt aggregierte Auswertungen/Berichte auf der Basis der bereitgestellten Daten für sich, Mercedes-Benz AG und den ASP. Ermöglicht die Übermittlung von transaktionsbezogenen Daten der B2B-Plattform, die für die oben genannten Prozesse verwendet werden können; erhält aggregierte Berichte ASP: Controller Ermöglicht die Übermittlung von transaktionsbezogenen Daten der B2B-Plattform, die für die oben genannten Prozesse verwendet werden können; erhält aggregierte Berichte	ISP-Daten: ISP-Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon, Bestelldaten (Bestelldatum, bestellte Teile/Dienstleistungen, Bestellmenge, Umsatz, nicht erteilte Aufträge (entgangener Umsatz), Häufigkeit der Nutzung von B2B Connect-Plattform-/Aftersales-bezogenen Diensten, Lieferzeiten) ASP-Daten: Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon

2. Empfänger

Eingeschränkte Personen mit speziellen Aufgaben, an die personenbezogene Daten nur dann weitergegeben werden, wenn dies für die Erfüllung ihrer jeweiligen Führungsaufgaben erforderlich ist (z. B. Auftragnehmer, einschließlich Personal-, IT- und Finanzabteilung (sofern zutreffend)); Konzernunternehmen, Berater, Wirtschaftsprüfer, Buchhalter; Finanzorganisationen; Strafverfolgungsbehörden, Regierungsbehörden, Aufsichtsbehörden.

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

TEIL B

Klauseln zur Datenverarbeitung im Auftrag eines Verantwortlichen

Präambel

Diese Klauseln über die Datenverarbeitung im Auftrag eines Verantwortlichen ("**Klauseln Teil B**") legen die Verpflichtungen der Parteien in Bezug auf den Datenschutz fest, die sich aus der Datenverarbeitung im Auftrag eines Verantwortlichen ergeben, wie nachstehend beschrieben. Diese Klauseln von Teil B gelten für jede Tätigkeit, die sich auf diese Verarbeitungen bezieht und bei der Mitarbeiter des Auftragsverarbeiters oder von ihm beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können. Die Anwendung dieser Klauseln ist jedoch auf Fälle beschränkt, in denen eine der Parteien gegenüber der anderen Partei als Auftragsverarbeiter im Sinne von Art. 28 DSGVO handelt. Außerhalb dieses Anwendungsbereichs finden diese Klauseln keine Anwendung.

1. Aufgaben und Zuständigkeiten

Der für die Verarbeitung Verantwortliche ist auf die Verarbeitung personenbezogener Daten angewiesen, um seine Aftersales-Dienstleistungen zu erbringen. Zu diesem Zweck erbringt der Auftragsverarbeiter die in Anhang 1 beschriebenen Dienstleistungen für den Verantwortlichen.

2. Gegenstand und Verantwortlichkeit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Gegenstand der Beauftragung sind die nachstehend oder in einer zusätzlichen Servicevereinbarung oder einem Auftragsformular genannten Tätigkeiten. Im Rahmen dieser Klauseln von Teil B ist der für die Verarbeitung Verantwortliche allein für die Einhaltung des geltenden Datenschutzrechts verantwortlich, insbesondere für die Rechtmäßigkeit der Übermittlung von Daten an den Auftragsverarbeiter, die Verarbeitung der Daten durch den Auftragsverarbeiter und jede weitere Verarbeitung von Daten im Rahmen der Dienstleistungen, während der Auftragsverarbeiter für die Einhaltung der für einen Auftragsverarbeiter geltenden gesetzlichen Datenschutzbestimmungen verantwortlich ist.

3. Spezifizierung der Beauftragung

3.1 Zweck, Art und Umfang der beauftragten Erhebung, Verarbeitung und/oder Nutzung von personenbezogenen Daten sind in Anhang 1 näher beschrieben.

3.2 Die Art und die Kategorien der gesammelten und/oder verwendeten personenbezogenen Daten sowie die Kategorie der betroffenen Personen, die Gegenstand der Verarbeitung personenbezogener Daten sind, werden in Anhang 1 näher beschrieben.

4. Weisungsrecht des Verantwortlichen

4.1 Der Verantwortliche behält sich im Rahmen der Beauftragung ein Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelanweisungen konkretisieren kann. Diese sind abschließend festgelegt und durch die Einstellungen und Funktionen, wie sie die bereitgestellten Anwendungen und Systeme bieten, auszuüben. Weisungen, die zu Änderungen des vereinbarten Verarbeitungsgegenstandes und der Verfahren führen, sind zu vereinbaren und zu dokumentieren.

4.2 Der Auftragsverarbeiter wird den Verantwortlichen über jede Weisung informieren, die seiner Meinung nach gegen die Anforderungen des Datenschutzes verstößt. Der Auftragsverarbeiter kann dann die Ausführung der betreffenden Weisung so lange zurückstellen, bis sie vom Verantwortlichen schriftlich (auch per E-Mail) bestätigt oder geändert wird.

4.3 Vorbehaltlich einer abweichenden schriftlichen Vereinbarung zwischen den Parteien sind auf Seiten des Verantwortlichen nur die Geschäftsführung oder sonstige vertretungsberechtigte Personen befugt, Weisungen zu erteilen, die der Schriftform (auch per E-Mail) bedürfen.

4.4 Bevollmächtigter für die Entgegennahme von Anweisungen seitens des Auftragsverarbeiters ist der "Datenschutzkoordinator für die Mercedes-Benz AG, Vertrieb Deutschland, der über mbvddatenschutz@mercedes-benz.com kontaktiert werden kann.

5. Pflichten des Auftragsverarbeiters

5.1 Der Auftragsverarbeiter erhebt oder verarbeitet Daten nur im Auftrag des Verantwortlichen und gemäß den Anweisungen des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist aufgrund von Rechtsvorschriften der Europäischen Union oder der Mitgliedstaaten oder aufgrund anderer anwendbarer Datenschutzgesetze, denen der Auftragsverarbeiter unterliegt, dazu verpflichtet; in einem solchen Fall unterrichtet der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über diese rechtlichen Anforderungen, es sei denn, diese Rechtsvorschriften verbieten eine solche Unterrichtung aus wichtigen Gründen des öffentlichen Interesses.

Der Auftragsverarbeiter wird die im Auftrag des Verantwortlichen verarbeiteten Daten nur auf Anweisung des Verantwortlichen berichtigen, löschen oder sperren. Wendet sich eine betroffene Person mit einem Antrag auf Berichtigung oder Löschung ihrer Daten an den Auftragsverarbeiter, so leitet dieser den Antrag an den Verantwortlichen weiter.

5.2 Sofern dies nicht durch geltende Rechtsvorschriften oder eine rechtsverbindliche Aufforderung der Strafverfolgungsbehörden untersagt ist, unterrichtet der Auftragsverarbeiter den Verantwortlichen unverzüglich über jedes Ersuchen einer Datenschutzaufsichtsbehörde, einer Strafverfolgungsbehörde oder einer anderen öffentlichen Stelle um Zugang zu oder Beschlagnahme von personenbezogenen Daten. Darüber hinaus muss der Auftragsverarbeiter, soweit dies gesetzlich zulässig ist, alle angemessenen Maßnahmen ergreifen, um sich gegen eine solche Klage zu verteidigen, oder dem Verantwortlichen gestatten, dies anstelle des Auftragsverarbeiters und in dessen Namen zu tun, und, falls er dies wünscht, eine Schutzanordnung beantragen oder dem Verantwortlichen gestatten, dies im Namen des Auftragsverarbeiters zu tun. In jedem Fall wird der Auftragsverarbeiter mit dem Verantwortlichen bei einer solchen Verteidigung angemessen zusammenarbeiten.

5.3 Bevor der Auftragsverarbeiter Zugang zu den personenbezogenen Daten gewährt, verpflichtet er die mit der Verarbeitung der personenbezogenen Daten befassten Personen auf das Datengeheimnis und die Vertraulichkeit und macht sie mit den Bestimmungen dieser Klauseln Teil B und den für sie geltenden Datenschutzpflichten vertraut. Soweit der Auftragsverarbeiter personenbezogene Daten verarbeitet, die dem Berufsgeheimnis oder anderen besonderen Vertraulichkeitsverpflichtungen unterliegen (z. B. Daten, die dem Fernmeldegeheimnis unterliegen), umfasst diese Verpflichtung auch diese besonderen Umstände und damit verbundenen Verpflichtungen.

5.4 Soweit es das geltende Datenschutzrecht erfordert, muss der Auftragsverarbeiter einen Datenschutzbeauftragten benennen und dessen Kontaktdaten an den Verantwortlichen weiterleiten und dem Verantwortlichen unverzüglich alle Änderungen und Aktualisierungen während der Laufzeit dieser Vereinbarung mitteilen.

5.5 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Verstöße des Auftragsverarbeiters oder eines Mitarbeiters des Auftragsverarbeiters gegen Anweisungen oder Bestimmungen zum Schutz der personenbezogenen Daten des Verantwortlichen informieren.

Der Auftragsverarbeiter nimmt zur Kenntnis, dass der für die Verarbeitung Verantwortliche verpflichtet sein kann, Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und erforderlichenfalls eine Aufsichtsbehörde bzw. die betroffene Person innerhalb von 72 Stunden über eine solche Verletzung zu informieren. Wenn und soweit es zu solchen Verletzungen gekommen ist, wird der Auftragsverarbeiter den Verantwortlichen gemäß Art. 28 Unterabsatz 3 Buchstabe f DSGVO bei der Erfüllung seiner Meldepflichten in angemessener Weise unterstützen, um dem Verantwortlichen die rechtzeitige Erfüllung seiner Pflichten zu ermöglichen. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über den Verstoß und übermittelt ihm zumindest die folgenden Informationen, sofern und soweit diese dem Auftragsverarbeiter zur Verfügung stehen: (a) Beschreibung der Art der Verletzung, die Kategorie und die ungefähre Anzahl der betroffenen Personen und Datensätze, (b) Name und Kontaktperson für weitere Informationen, (c) Beschreibung der wahrscheinlichen Folgen der Verletzung, (d) Beschreibung der Maßnahmen, die ergriffen wurden, um die Verletzung zu beheben oder zu verringern.

Der Auftragsverarbeiter ist ferner verpflichtet, den Verantwortlichen unverzüglich über schwerwiegende Störungen des normalen Betriebsablaufs, den Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen zu informieren.

5.6 Der Auftragsverarbeiter informiert den Verantwortlichen über alle Überwachungsaktivitäten und Maßnahmen der Aufsichtsbehörde in Bezug auf die Verarbeitung personenbezogener Daten des Verantwortlichen.

5.7 Der Auftragsverarbeiter unterstützt den Verantwortlichen im Sinne von Art. 28 Unterabsatz 3 Buchstabe e durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich und zumutbar ist, zur Erfüllung der Pflichten des Verantwortlichen gegenüber den betroffenen Personen (auch gemäß Kapitel II der DSGVO), z. B. Information und Auskunft der betroffenen Personen, Berichtigung und Löschung von Daten, Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und ggf. Widerspruchsrecht.

5.8 Der Auftragsverarbeiter unterstützt gemäß Art. 28 Unterabsatz 3 Buchstabe f DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und unterstützt ggf. die vorherige Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO. Auf Verlangen des Verantwortlichen legt der Auftragsverarbeiter dem Verantwortlichen die erforderlichen Informationen und Unterlagen vor.

5.9 Über die gemäß 5.7 und 5.8 anfallenden Mehrkosten werden sich die Vertragspartner verständigen. Eine Kostentragungspflicht für solche von Mercedes-Benz AG zu erbringenden Leistungen, zu deren Erbringung Mercedes-Benz AG unabhängig vom Bestehen dieses gesetzlichen Auftrags verpflichtet ist oder wäre, besteht nicht.

5.10 Der Auftragsverarbeiter hat die Einhaltung der oben genannten Pflichten bei der Durchführung der Auftragsdatenverarbeitung zu überwachen.

5.11 Der Auftragsverarbeiter führt ein Verzeichnis der im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten.

6. Sicherheit der Verarbeitung

6.1 Der Auftragsverarbeiter trifft alle geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten und den Verantwortlichen bei der Einhaltung der anwendbaren Datenschutzgesetze zu unterstützen.

Der Auftragsverarbeiter wird daher in seinem Verantwortungsbereich seine interne Organisation in Übereinstimmung mit allen geltenden Datenschutz- und Datensicherheitsanforderungen einrichten. Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu ergreifen, aufrechtzuerhalten und zu kontrollieren, um einen angemessenen Schutz der Daten des Verantwortlichen gegen Missbrauch und Verlust gemäß den Anforderungen der geltenden Gesetze zu gewährleisten.

6.2 Dabei hat der Auftragsverarbeiter ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, das dem Stand der Technik, den Implementierungskosten und der Art, dem Umfang, dem Kontext und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen Rechnung trägt. Dazu gehören geeignete Maßnahmen wie z. B. Zugangskontrolle, Benutzerkontrolle, Zugriffskontrolle, Übermittlungskontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie die Trennung nach Zwecken und ggf. die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten fortlaufend zu gewährleisten, die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen, sowie ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

6.3 Weitere Vorgaben zu den technischen und organisatorischen Maßnahmen ergeben sich aus Anhang 2.

6.4 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Entwicklung. Der Auftragsverarbeiter kann angemessene Ersatzmaßnahmen ergreifen. Diese dürfen jedoch nicht hinter dem Sicherheitsniveau der festgelegten Maßnahmen zurückbleiben. Wesentliche Änderungen sind jedoch zu dokumentieren.

7. Rechte und Pflichten des Verantwortlichen

7.1 Verantwortlicher und Auftragsverarbeiter sind bezüglich der im Rahmen dieses Vertrags zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzvorschriften verantwortlich.

7.2 Die betroffenen Personen haben verschiedene Rechte in Bezug auf die von dem Verantwortlichen (und dem Auftragsverarbeiter in seinem Namen) gespeicherten Daten. Da in jedem Fall auch der für die Verarbeitung Verantwortliche eine direkte Beziehung zu der betroffenen Person unterhält, muss der für die Verarbeitung Verantwortliche sicherstellen, dass die Rechte der betroffenen Personen ordnungsgemäß erfüllt werden, insbesondere dass die betroffenen Personen ordnungsgemäß über die Rollen und Aufgaben der Parteien im Einklang mit den geltenden Datenschutzgesetzen informiert werden, z. B. indem den Kunden Zugang zur aktuellen Fassung der einschlägigen Datenschutzrichtlinie gewährt wird.

7.3 Der Verantwortliche legt die Maßnahmen zur Rückgabe der überlassenen Datenträger bzw. zur Löschung der aufgenommenen Daten nach Beendigung der Beauftragung fest. Werden keine Vorgaben gemacht, sind die Daten an den Verantwortlichen zu übergeben oder zu vernichten. Soweit Daten nach bestimmten Vorgaben gelöscht werden, bestätigt der Auftragsverarbeiter dem Verantwortlichen die Löschung unter Angabe des Datums, an dem die Löschung erfolgt ist, auf Anfrage des Verantwortlichen.

8. Prüfung

8.1 Der Verantwortliche oder sein Beauftragter sind berechtigt, die Einhaltung aller in dieser Vereinbarung und im geltenden Datenschutzrecht festgelegten Anweisungen und Anforderungen zu prüfen, darunter auch durch regelmäßige Überprüfungen. Der Auftragsverarbeiter verpflichtet sich, solche Kontrollen zuzulassen und den Verantwortlichen zu unterstützen sowie die erforderlichen Informationen zur Verfügung zu stellen.

8.2 Der für die Verarbeitung Verantwortliche kommt seinen Kontrollpflichten in erster Linie dadurch nach, dass er entsprechende Selbstprüfungen durch den Datenschutzbeauftragten der Datenschutzorganisation des Auftragsverarbeiters und/oder Zertifizierungen durch unabhängige Prüfer verlangt. Der Verantwortliche behält sich das Recht vor, zusätzliche Vor-Ort-Prüfungen durchzuführen, wenn dies datenschutzrechtlich erforderlich ist.

8.3 Prüfungen durch den Verantwortlichen gemäß den Abschnitten 8.1 und 8.2 finden während der üblichen Geschäftszeiten statt, dürfen den normalen internen Betrieb nicht stören und müssen in angemessener Zeit im Voraus angekündigt werden.

8.4 Auf schriftliches Ersuchen des Verantwortlichen erteilt der Verarbeiter dem Verantwortlichen innerhalb eines angemessenen Zeitraums alle für die Prüfung erforderlichen Auskünfte und stellt die erforderlichen Unterlagen zur Verfügung.

9. Unterauftragsverarbeiter

9.1 Der Auftragsverarbeiter ist berechtigt, zur Erfüllung seiner vertraglichen Pflichten Unterauftragsverarbeiter einzusetzen.

9.2 Der Auftragsverarbeiter stellt durch den Abschluss von Vereinbarungen mit Unterauftragsverarbeitern sicher, dass den Unterauftragsverarbeitern zumindest im Wesentlichen die gleichen Verpflichtungen auferlegt werden, die der Auftragsverarbeiter gemäß diesen Klauseln IN Teil B übernommen hat, bevor dem Unterauftragsverarbeiter während der Ausführung Zugang zu den personenbezogenen Daten des Verantwortlichen gewährt wird.

9.3 Soweit der Auftragsverarbeiter Unterauftragsverarbeiter einbezieht, enthält Anhang 1 bestimmte weitere Angaben zu den beteiligten Unterauftragsverarbeitern je Verfahren. Zusätzlich sind die derzeit beteiligten Unterauftragsverarbeiter in Anhang 3 aufgeführt. Der Auftragsverarbeiter unterrichtet den Verantwortlichen über alle beabsichtigten Änderungen, die die Hinzufügung oder den Austausch anderer Unterauftragsverarbeiter betreffen, und gibt dem Verantwortlichen die Möglichkeit, gegen diese Änderungen Einspruch zu erheben, wobei der für die Verarbeitung Verantwortliche angemessene Gründe für einen solchen Einspruch vorlegen muss. Stimmt der Verantwortliche einem neuen Unterauftragsverarbeiter immer noch nicht zu, so können der Verantwortliche und der Auftragsverarbeiter die betroffenen Teile der Dienstleistungen ohne Vertragsstrafe durch schriftliche Kündigung beenden.

9.4 Dieser Abschnitt 9 findet keine Anwendung, wenn der Auftragsverarbeiter Nebenleistungen an Dritte vergibt; zu diesen Nebenleistungen gehören unter anderem Post-, Kommunikations-, Versand- und Empfangsdienste sowie Hausmeisterdienste.

10. Gebiet und internationale Datenübermittlung

10.1 Die Verarbeitung erfolgt in der Regel in einem Mitgliedsstaat der Europäischen Union, in einem Land des Europäischen Wirtschaftsraums oder in einem Land mit angemessenem Datenschutzniveau. Verarbeitungstätigkeiten in einem anderen Land ("Drittland") sind zulässig, wenn die geltenden Voraussetzungen für die internationale Übermittlung von personenbezogenen Daten erfüllt sind.

10.2 Soweit internationale Datenübermittlungen (einschließlich ggf. Datenübermittlungen in Bezug auf Unterauftragsverarbeiter) nicht von der Konzerndatenschutzrichtlinie EU A 17.4 von Mercedes-Benz erfasst werden, müssen die Parteien (auch in Bezug auf Unterauftragsverarbeiter) die entsprechenden EU-Standardvertragsklauseln vereinbaren.

10.3 Soweit anwendbar, haben die Bestimmungen der EU-Standardvertragsklauseln (einschließlich ihrer Anhänge) Vorrang vor allen widersprüchlichen Klauseln in den übrigen Teilen dieser Klauseln Teil B und der gesamten Vereinbarung. Zur Vermeidung von Zweifeln bleiben Bestimmungen in den übrigen Teilen dieser Klauseln Teil B sowie der gesamte

Vereinbarung, die lediglich über die Bestimmungen der EU-Standardvertragsklauseln hinausgehen, ohne diesen zu widersprechen, gültig.

11. Haftung

Unbeschadet des Abschnitts 7 im Hauptteil dieses Vertrags haftet der Verantwortliche für Schäden und stellt den Auftragsverarbeiter von allen Ansprüchen Dritter oder sonstigen Schäden und Verbindlichkeiten frei, darunter auch die Folgen von Anordnungen der Aufsichtsbehörden oder Bußgelder, die zurückzuführen sind auf (i) den Verstoß des Verantwortlichen gegen seine Verpflichtungen im Rahmen dieses Vertrages oder sonstiger Verstößen gegen geltende Datenschutzvorschriften und/oder (ii) den Verstoß des Auftragsverarbeiter gegen geltende Datenschutzvorschriften, soweit diese auf der ordnungsgemäßen Durchführung der Bestimmungen dieses Vertrags oder sonstiger Anweisungen des Verantwortlichen beruhen. Dies gilt nicht, wenn der Verantwortliche die haftungsauslösenden Umstände nicht zu vertreten hat.

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Anlage 1: Rollen, Aufgaben und Umfang der Zusammenarbeit

1. B2B Connect-bezogene Verarbeitungstätigkeiten

Verfahren	**Zweck/ Umfang**	**Rollen und Aufgaben**	**Datenkategorien und betroffene Personen**
Systemsupport für B2B Connect-Plattformdienste	Benutzerunterstützung für Mitarbeiter des ASP (über Ticketing Tool / Call Center)	MBAG : Auftragsverarbeiter Bietet Unterstützung für ASPs bzw. ASP: Controller Verwendung von WebParts einschließlich Benutzerunterstützung	ASP-Daten: Kontodaten, einschließlich Kundenname/Firmenname, Name des Kundenmitarbeiters und Kundenkontaktdaten, Kundenadresse, Informationen über Support-Tickets/Vorfälle, Informationen über Kundendienstleistungen, Systemnutzungsdaten, einschließlich Transaktionsdaten und damit verbundene ISP-Daten, einschließlich ISP-Firmentitel, Mitarbeiternamen oder auftragsbezogene Daten (sofern erforderlich)

2. Business Analytics

Verfahren	**Zweck/ Umfang**	**Rollen und Aufgaben**	**Datenkategorien und betroffene Personen**
Anzeige, Berichtswesen und Analytik	Anzeige von ISP-Transaktionsdaten im B2B Connect Seller Center, Bereitstellung von Berichten und Analysen	MBAG: Auftragsverarbeiter Anzeige von ISP-Transaktionsdaten im B2B Connect Seller Center und Bereitstellung von Berichten und Analysen auf Anfrage des ASP ASP: Controller Verwendung von WebParts, einschließlich Datenanzeige, Berichten und Analysen	ISP-Daten: ISP-Firmenname, Benutzername, Benutzer-ID, Bestelldaten (Bestelldatum, bestellte Teile/Dienstleistungen, Bestellmenge, Umsatz, nicht erteilte Aufträge (entgangener Umsatz), Häufigkeit der Nutzung von B2B Connect / Aftersales-bezogenen Diensten, Lieferzeiten), Analysen und Berichte auf Basis vorstehender Umsatzzahlen ASP-Daten: Firmenname, Benutzername, Benutzer-ID
Kampagnenvorschlagsdienste (falls ein solcher Dienst vom ASP angefordert wird; ansonsten nicht anwendbar)	MBAG verwendet die zur Verfügung gestellten Daten zur Durchführung von Geschäftsanalysen und zur Erstellung von entsprechenden eigenen und Marketingkampagnen der ASPs sowie zur Unterstützung bei der Durchführung von Marketingkampagnen. Dies beinhaltet typischerweise, dass MBAG ASPs Marketingmaterialien einschließlich ISP-Listen (z. B. mit Leads) zur Verfügung stellt, um diesen zu ermöglichen, ISPs über verschiedene Direktmarketing-Kanäle zu kontaktieren (falls im jeweiligen Markt anwendbar), einschließlich der	MBAG: Auftragsverarbeiter Hostet eine Datenbank mit Geschäftsanalysedaten; betreibt Anwendungen und erstellt auf der Grundlage der bereitgestellten Daten Marketingkampagnen ASPs, damit diese über verschiedene Direktmarketingkanäle mit ISPs in Kontakt treten können. Übermittlung von Marketingmaterial + ISP-Listen ASPs zu diesem Zweck. MBAG: Controller	ISP-Daten: ISP-Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon, Bestelldaten (Bestelldatum, bestellte Teile/Dienstleistungen, Bestellmenge, Umsatz, nicht erteilte Aufträge (entgangener Umsatz), Häufigkeit der Nutzung von B2B Connect-Plattform-/Aftersales-bezogenen Diensten, Lieferzeiten) ASP-Daten: Firmenname, Benutzername, Benutzer-ID, Adresse, E-Mail, Telefon

	Übermittlung von Marketingmaterialien + Händlerlisten an ASPs zu diesem Zweck.	Marketingkampagnen werden in alleiniger Verantwortung von MBAG durchgeführt) Kann ähnliche Dienste für ASPs bereitstellen (in diesem Fall auch als Verarbeiter für ASPs) ASP: Controller Erhalt von ISP-Listen und Marketingmaterial für Marketingkampagnen (Marketingkampagnen werden vom ASP in alleiniger Verantwortung durchgeführt)	
Dienste für Direktmarketing-Kampagnen (falls ein solcher Dienst vom ASP angefordert wird; ansonsten nicht anwendbar)	Optional kann MBAG im Auftrag eines ASP den Versand von Marketingmaterial an Kunden unterstützen, indem ein spezieller Web-Service für ASPs bereitgestellt wird, mit dem Endkunden-Kontaktdaten hochgeladen werden können und Mercedes-Benz AG Kampagnen im Namen und im Auftrag des ASP verteilt. Mercedes-Benz AG kann ASPs zudem Marketingunterstützung durch Kontaktaufnahme zu ISPs über das Mercedes-Benz-Callcenter leisten.	MBAG: Auftragsverarbeiter MBAG kann im Namen und im Auftrag des ASP (oder unter Einbeziehung eines anderen Unterauftragsverarbeiters) Marketingkampagnen (E-Mails) versenden. MBAG verarbeitet die übermittelten Daten dann für den Versand von Marketing-E-Mails (auch über Drittdienstleister von Mercedes-Benz AG). MBA kann optional ISPs auch über das Mercedes-Benz-Callcenter kontaktieren, um in Bezug auf frühere geschäftliche Transaktionen nachzufassen. ASP: Controller Führt Marketingkampagnen durch	ASP-Daten: Firmenname, Mitarbeitername, Benutzer-ID, Adresse, E-Mail, Telefon ISP-Daten: Firmenname, Kontaktdaten, Namen der Mitarbeiter, E-Mail, Bestelldaten (Datum der Bestellung, bestellte Teile/Dienstleistungen, Bestellmenge, Umsatz, nicht erteilte Aufträge (entgangener Umsatz), Häufigkeit der Nutzung von B2B Connect-Plattform-/Aftersales-bezogenen Diensten, weitere Lead-bezogene Informationen

3. Empfänger

Eingeschränkte Personen mit speziellen Aufgaben, an die personenbezogene Daten nur dann weitergegeben werden, wenn dies für die Erfüllung ihrer jeweiligen Führungsaufgaben erforderlich ist (z. B. Auftragnehmer, einschließlich Personal-, IT- und Finanzabteilung (sofern zutreffend)); Konzernunternehmen, Berater, Wirtschaftsprüfer, Buchhalter; Finanzorganisationen; Strafverfolgungsbehörden, Regierungsbehörden, Aufsichtsbehörden.

Anhang 2: Technische und organisatorische Maßnahmen

Im Folgenden sind die technischen und organisatorischen Maßnahmen zu dokumentieren, die vom Auftragsverarbeiter für die Gewährleistung der Sicherheit der Datenverarbeitung umgesetzt werden.

Es erfolgt eine Ermittlung der mit der Datenverarbeitung verbundenen Risiken durch u.a. die Risikoevaluierung (Schwellwertanalyse) sowie daraus abgeleiteten technischen- und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit. Die Festlegung der technischen Maßnahmen zur Gewährleistung der Datensicherheit erfolgen unter Berücksichtigung des Stands der Technik als auch der Implementierungskosten. Beim Stand der Technik handelt es sich um bewährte und effektive Maßnahmen, die derzeit auf dem Markt verfügbar sind; Konkretisierung bieten anerkannte nationale oder internationale Standards (z.B. von BSI, ENISA, NIST, TeleTrust).

Die fortlaufende Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen, z.B. DSGVO, BDSG, GoB, wird durch das „IT-Sicherheitsmanagement" sichergestellt, wo neben Definitionen und Funktionen, sowie Aufgaben und Verantwortlichkeiten auch u.a. die nachfolgend in dieser Anlage durchgeführten technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO umgesetzt und im Rahmen von Sicherheitschecks überprüft, bewertet und im Hinblick auf ihre Wirksamkeit evaluiert werden.

Die nachfolgend beschriebenen Maßnahmen stellen die Auswahl der technischen und organisatorischen Maßnahmen („TOM") zur Gewährleistung der Datensicherheit nach Art. 32 DSGVO passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik dar. Die konkreten umzusetzenden TOM richten sich nach der jeweiligen Schutzstufe.

Dabei wurde das nachfolgende Schutzstufenkonzept zugrunde gelegt:

Schutz-Stufe (SF)	*Personenbezogene Daten,*	*zum Beispiel (für einzelne Daten; bei Kumulierung von Daten ggfs. höhere Schutzstufe angebracht!)*	*Schwere des möglichen Schadens*
A	die vom Betroffenen frei zugänglich gemacht worden sind	Telefonverzeichnis, frei zugängliche Webseite, frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von dem Betroffenen	Beschränkt zugängliche öffentliche Dateien, Grundbucheinsicht, nicht frei zugängliche soziale Medien; maskierte IBAN (die letzten	geringfügig

	nicht frei zugänglich gemacht wurden	sechs Zahlen geschwärzt), Kundenstammdaten, Geburtsdatum, Geburtsort	
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“)	Einkommen, Steuerdaten, Ordnungswidrigkeiten, Passdaten, IBAN (vollständig); Vertragsdaten (Liefer- und Bestelldaten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“)	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Daten besonderer Kategorien nach Art. 9 DS-GVO	substanziell
E	Deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß
F	die im Rahmen der Fernwartung / des Fernzugriffs verarbeitet werden	Sonderregelungen, die auf die spezifische Situation der Fernwartung / Fernzugriff eingehen.	

Die Parteien haben festgestellt, dass die in diesem Auftragsverarbeitungsvertrag geregelte Verarbeitung personenbezogener Daten dem folgenden Schutzbedarf unterliegt:

Schutzstufe	Zutreffendes ankreuzen
A	☐
B	☒
C	☐
D	☐
E	☐

F	☐

Die einzelnen technischen und organisatorischen Maßnahmen sind zur Übersichtlichkeit ihren primären Schutzzielen, der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten, zugeordnet. Organisatorische und prozessuale Schutzmaßnahmen unterstützen die primären Schutzziele. Diese Übersicht enthält ausgewählte und repräsentative Zuordnungen der angeführten IT-Sicherheitsmaßnahmen zu den vorab genannten Schutzstufen als Empfehlung. Diese können, um eine Flexibilität bei der Auswahl angemessener Maßnahmen auch ergänzt oder ersetzt werden. Sofern für einzelne Datenverarbeitungen ein Schutzbedarf nach Schutzstufe E festgestellt worden ist, werden die zusätzlich getroffenen Maßnahmen zur Gewährleistung der Schutzziele in der jeweiligen Verfahrensbeschreibung dokumentiert.

Zum Nachweis der Umsetzung von angemessenen technischen und organisatorischen Maßnahmen kann, in Abhängigkeit des Risikos der Verarbeitung, ein nach der DSGVO durchgeführtes Zertifizierungsverfahren als Faktor herangezogen.

	TOM MB AG inkl. Schutzstufenempfehlung	
1. Vertraulichkeit der Systeme und Dienste	*Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen; vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.*	
1.1 Physischer Schutz der Vertraulichkeit	*Festlegung und Dokumentation zutrittsberechtigter Personen, einschließlich des Umfanges der Berechtigung (SF Empfehlung A B C D F)*	☐
	Existenz von Zutrittsregeln-Regelungen für Firmenfremde (SF Empfehlung A B C D F)	☐
	Zutrittsschutz in Form einer äußeren Umschließung/Umfriedung	☐
	Umsetzung einer Schlüsselregelung (SF Empfehlung A B C D F)	☐
	Protokollierung der ein- und ausgehenden Personen (SF Empfehlung C D)	☐

	Freiland-Sicherungsmaßnahmen (wie z.B. Geländegestaltung, Zufahrtssperren, Beleuchtung, Videoüberwachung und Detektionssensorik) (SF Empfehlung A B C D F)	☐
	Ausgabe von Zutrittsberechtigungsausweisen (SF Empfehlung C D)	☐
	Ausweispflicht bzw. offenes Tragen von Dienstausweisen auf dem Betriebsgelände und deren Liegenschaften	☐
	Pforten- und Empfangspersonal während der Betriebszeiten (SF Empfehlung C D)	☐
	Wach- und Schließdienst für Liegenschaften außerhalb der Betriebszeiten	☐
	Physische Schutzmaßnahmen sind vorhanden und werden regelmäßig überprüft:	☐
	gesicherter Eingang durch Ausweisleser (SF Empfehlung A B C D F)	☐
	einbruchhemmende Fenster (SF Empfehlung C D)	☐
	Gerätesicherung gegen Diebstahl, physische Manipulation und Beschädigung	☐
	Überwachungseinrichtung (z.B. Alarmanlage, Videoüberwachung)	☐
	Vereinzelungsanlagen (z.B. Drehkreuz, Schleuse) (SF Empfehlung C)	☐
	Unterteilung in verschiedene Sicherheitszonen	☐
	Arbeitsplatzrechner sind in verschlossenen Räumen	☐
	Räume mit Servern sind alarmüberwacht	☐
	Maßnahmen gegen einfaches Mithören und Einsichtnahme	☐
	Ausdruck-Erstellung an definierte Gebäude-Zonen gebunden oder durch persönliches Drucken (z.B. Print-to-me, follow-me print, mit PIN)	☐

	Aktenvernichtung ausschließlich innerhalb definierter Zonen (z.B. durch Schredder)	☐
	Bei Serverräumen mit mehreren Nutzern sind Hardware(-Schnittstellen) durch verschlossene Racks, verschlossene Schränke oder verschlossene Käfige sichergestellt	☐
	Bewegungs-Sensoren, Glasbruch-Sensoren oder Bilderkennung	
	Unverzügliche Abarbeitung der Alarmmeldungen nach Alarmplan	☐
	Dauerhafte Überwachung von Fluchttüren	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollten physische Schutzmaßnahmen für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: *Physische Schutzmaßnahmen gemäß Mercedes-Benz Group AG Standard*	
1.2 Schutz des Systemzugangs	*Angemessener Passwortschutz (verbindliche dokumentierte Vorgaben)* *(SF Empfehlung A B C D F)*	☒
	(System-)Passwörter werden nicht im Klartext gespeichert	☒
	(System-)Passwörter werden nach dem Stand der Technik gehashed gespeichert	☒
	Konzeption und Implementierung eines Berechtigungskonzepts (SF Empfehlung A B C D F)	☒
	Berechtigungskonzept für Endgeräte (Rechner)	☒
	Berechtigungskonzept für IT-Applikationen/IT-Systemen	☒
	Weitere Interaktionen mit dem IT-System sind nur nach einer erfolgreichen Authentifizierung möglich *(SF Empfehlung A B C D F)*	☒

	Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen und mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugriffsmöglichkeit aus dem Internet)	☒
	Authentisierungsverfahren am Schutzbedarf der Informationen orientiert (Klassifizierung):	☒
	Zugangsfunktion über Hardware-Token	☒
	Zwei-Faktorauthentifizierung (SF Empfehlung C D F)	☒
	Drei-Faktorauthentifizierung	☒
	Für die Administration des oder der IT-Systeme werden ausschließlich starke Passwörter mit mindestens 16 Zeichen verwendet	☐
	Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)	☒
	Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle	☒
	Spezielle Sicherheitssoftware (z.B. Anti-Malware-SW, VPN, Firewall)	☒
	Eine Segmentierung der genutzten Netze ist definiert	☐
	Regeln und Verfahren zur Netzwerksegmentierung sind definiert und umgesetzt	☐
	Aktenvernichter/-schredder (mind. Stufe 3, cross cuting)	☒
	Externer Aktenvernichter (DIN 32757)	☒
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Zugangskontrolle für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an:	

1.3Berechtigungsmanagement (stützt auch das Schutzziel der Integrität)	*Die Verwendung von eindeutigen und personalisierten Benutzerkonten ist festgelegt (SF Empfehlung A B C D)*	☒
	Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer	☒
	Berechtigungs- und Rollenkonzept für IT-Applikationen/IT-Systeme sind dokumentiert und umgesetzt (SF Empfehlung A B C D)	☒
	Zugriffsberechtigungen und -beschränkungen gemäß „Need-to-Know“ und „Least Privilege“ (SF Empfehlung A B C D)	☒
	Regelmäßige Überprüfung der Berechtigungen (SF Empfehlung A B C D F)	☒
	Berechtigungsprüfung und Kontrolle der Zugangsbefugnisse aller Benutzer erfolgt auch innerhalb eines IT-Systems (z.B. Modul, Tabelle, Datensatz)	☒
	Revisionssichere Dokumentation von Benutzerberechtigungen	☒
	Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess nach dem 4-Augen-Prinzip (SF Empfehlung A B C D)	☒
	Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)	☒
	Die Nutzung von "Sammel-Konten" ist geregelt (z. B. eingeschränkt, nur wenn auf den Nachweis der Handlungen verzichtet werden kann)	☐
	Benutzerbezogene Zugänge zu Daten des Verantwortlichen dürfen nicht von mehreren Benutzern verwendet werden	☒
	Ein Basis-Benutzerkonto mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet	☐

	Veränderungen der Zuständigkeiten von Mitarbeitern oder dem Arbeitsverhältnis mit diesen werden dem Systemadministrator umgehend mitgeteilt oder die Benutzerzugänge werden entsprechend angepasst	☒
	Protokollierung von Events (SF Empfehlung A B C D)	☒
	Protokollierung des lesenden Zugriffs	☒
	Protokollierung des schreibenden Zugriffs (inkl. Löschung/Überschreiben)	☒
	Protokollierung von unberechtigten Zugriffsversuchen	☐
	Regelmäßige Auswertung Anlassbezogene Auswertung	☐
	Ein Management-Prozess (Vergabe/Änderung/Löschung) für privilegierte Benutzerkennungen ist dokumentiert und etabliert (SF Empfehlung A B C D)	☒
	Die Vergabe von privilegierten Rechten erfolgt erst nach ausdrücklicher dokumentierter Genehmigung (SF Empfehlung A B C D)	☒
	Es werden sichere Authentifizierungsverfahren für privilegierte Benutzerkonten verwendet	☒
	Benutzerkonten mit privilegierten Rechten sind dokumentiert und werden regelmäßig überprüft	☒
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Zugriffskontrolle für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an:	
1.4 Verschlüsselung	*Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik*	☒

Kommentiert [SG(1]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(2]: @GCSP/BW: Bitte Begründung angeben.

	Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert	☒
	Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert	☒
	Übermittlung von personenbezogenen Daten erfolgt ausschließlich verschlüsselt, unter Verwendung von Verschlüsselungsverfahren nach dem Stand der Technik (SF Empfehlung A B C D F)	☐
	Verschlüsselte Speicherung von personenbezogenen Daten (SF Empfehlung A B C D)	☐
	Ein Regelwerk mit Anforderungen an die Verschlüsselungsstärke, die Verwaltung der Schlüssel, dem Verschlüsselungsalgorithmus ist dokumentiert und umgesetzt (SF Empfehlung C D)	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, insbesondere wenn die verschlüsselte Übermittlung nach dem Stand der Technik nicht garantiert werden kann, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Verschlüsselung für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: Keine personenbezogenen Daten verarbeitet	
1.5 Pseudonymisierung	*Pseudonymisieren durch Einwegfunktionen*	☐
	Pseudonymisieren durch Zuordnungstabellen:	☐
	Zugriffe werde differenziert nach Lesen, Schreiben, Löschen (auf dem IT-System, das die Zuordnungstabellen verwaltet) in Protokollen dokumentiert	☐
	Zuordnungstabellen sind organisatorisch von Kernbetrieb der in Rede stehenden Datenverarbeitung getrennt	☐

Kommentiert [SG(3]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(4]: @GCSP/BW: Bitte Begründung angeben

	Falls Sie Einwegfunktionen zur Pseudonymisierung nutzen spezifizieren Sie den oder die genutzten Hash-Verfahren in folgendem Freitextfeld:	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Pseudonymisierung für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: *Pseudonymisierung nicht erforderlich, da keine Verarbeitung personenbezogener Daten*	
2. Integrität der Systeme und Dienste	*Eine unerlaubte oder unbeabsichtigte Veränderung stellt eine Verletzung der Integrität von Informationen dar; dies kann neben dem eigentlichen Inhalt auch Attribute wie den Urheber oder Absender sowie den Zeitpunkt der Erstellung betreffen. Integrität kann sich sowohl auf die Unversehrtheit von Daten als auch auf die korrekte Funktionsweise von Systemen beziehen.*	
2.1 Schutz der Datenübertragung (stützt auch das Schutzziel der Vertraulichkeit)	*Vollständige Dokumentation der Wege der Weitergabe von personenbezogenen Daten im Zuge dieser Auftragsverarbeitung (z.B. Ausdruck, Datenträger, automatisierte Übermittlung, WAN-Strecke, TLS)* *(SF Empfehlung A B C D)*	☐
	Definition und Dokumentation der Empfänger von personenbezogenen Daten im Kontext der hier vereinbarten Auftragsverarbeitung	☐
	Sicherungen des Transports (z.B. sicheres Fahrzeug, Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle, TLS-verschlüsselte Übermittlung) *(SF Empfehlung A B C D F)*	☐
	Dokumentationen aller Schnittstellen und der Abruf- und Übermittlungsprogramme	☒

Kommentiert [SG(5]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(6]: @GCSP/BW: Bitte Begründung angeben.

	Es werden elektronische Signaturverfahren eingesetzt	☐
	Es werden qualifizierte elektronische Signaturen eingesetzt	☐
	Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen: *(SF Empfehlung B C D)*	☐
	Deaktivierung von USB-Schnittstellen	☐
	Beschränkung der Befugnisse zur Datenübertragung	☐
	Regelmäßige Kontrolle der zulässigen Empfänger	☒
	Technische Beschränkung auf zulässige Empfänger	☒
	Bei Massen-E-Mailversand wird die Offenlegung aller Empfänger technisch oder organisatorisch verhindert	☐
	Data Loss Prevention Lösungen werden eingesetzt	☐
	Durchführung von Protokollierungen einer elektronischen Datenweitergabe oder Übermittlung Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen	☒
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
2.2. Eingabekontrolle	*Protokollierung der Eingaben von und Änderungen an personenbezogenen Daten*	☐
	Regelmäßige Überprüfung der Protokolle zu Eingaben/Änderungen personenbezogener Daten	☐
	Organisatorisch festgelegt Zuständigkeiten für die Eingabe *(SF Empfehlung A B C D)*	☒
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen	

Kommentiert [SG(7]: @GCSP/BW: Bitte befüllen

	Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Eingabekontrolle für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: *Keine personenbezogenen Daten werden verarbeitet*	
2.3 Weitere Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste	*Das Minimalprinzip wird eingehalten (z. B. Einschränkung der Berechtigungen, Ports, Protokolle, Software)*	☒
	Es erfolgt eine automatische Überprüfung der von zentralen Gateways transportierten Daten (z.B. E-Mail, Internet, Netze von Dritten) mittels einer Schutzsoftware (inkl. verschlüsselter Verbindungen)	☐
	Mandantenfähigkeit: *(SF Empfehlung A B C D)*	☐
	Dedizierte physische Server	☐
	Trennung auf Systemebene *(SF Empfehlung A B C D)*	☐
	Trennung auf Datenebene	☐
	Beschreibung der Umsetzung der Mandantentrennung	☐
	Es ist sichergestellt, dass durch eine wirksame Trennung unbefugte Nutzer von Organisationen nicht auf personenbezogene Daten anderer Organisationen zugreifen können	☐
	Dateneingaben werden nach semantischen Kriterien validiert (semantic input validation)	☐
	Gemeinsam genutzte virtuelle Maschinen und/oder Applikationsinstanzen sind entsprechend gehärtet	☒
	Eine Separierung von Daten, Applikationen, Betriebssystem, Storage und Netzwerk ist umgesetzt	☒

Kommentiert [SG(8]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(9]: @GCSP/BW: Bitte Begründung angeben

	Dedizierte physische Leitungen zur Datenübertragung Eigene virtuelle Leitungen zur Datenübertragung	☐
	Es erfolgt eine automatische Überprüfung von empfangenen Dateien und Programmen vor deren Ausführung auf Schadsoftware (On-Access-Scan)	☐
	Es erfolgt eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware	☐
	Es existiert ein Intrusion Detection System	☐
	Es existiert ein Intrusion Prevention System	☐
	Zweckattribute sind für Datenfelder und –sätze definiert und umgesetzt worden	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollten die oben aufgezählten Maßnahmen für die hier beauftragte Auftragsverarbeitung nicht relevant sein, geben Sie hier eine kurze Begründung dafür an:	
3. Verfügbarkeit der Systeme und Dienste	*Verfügbarkeit von [Daten,] Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen bedeutet, dass diese von den Anwendern stets wie vorgesehen genutzt werden können.*	
3.1 Sicherung der Verfügbarkeit personenbezogener Daten Anmerkung: Die Sicherung der Verfügbarkeit Personenbezogener	*Vorhandensein von redundanten IT-Systemen (Endgeräte, Server, Speicher etc.)*	☐
	Unterbrechungsfreie Stromversorgung (USV) (SF Empfehlung A B C D)	☐
	Funktionsfähige physische Schutzeinrichtungen für Brandschutz, Energieversorgung, Klimatisierung) (SF Empfehlung C D)	☐

Kommentiert [SG(10]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(11]: @GCSP/BW: Bitte Begründung angeben

Daten stützt auch das Schutzziel der Integrität.	*Serverräume und Rechenzentren verfügen über Feuer- und Rauchmeldeanlagen (SF Empfehlung A B C D)*	☐
	Serverräume und Rechenzentren verfügen über Feuerlöscher bzw. Feuerlöschanlagen	☐
	Serverräume und Rechenzentren verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit	☐
	Regelmäßige Kontrollen des Systemzustandes (Monitoring)	☐
	Vorhandensein von divers ausgelegten IT-Systemen (gleiche Funktionalität von unterschiedlichen Herstellern)	☐
	Durchführung von regelmäßigen Bestandskontrollen für Ausdrucke und Datenträger	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Sicherung der Verfügbarkeit für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: Keine personenbezogene Daten werden verarbeitet	
3.2 Löschung	*Definition und Dokumentation von Löschfristen für Daten (Löschkonzept)*	☒
	Umsetzung der Löschung gemäß der Löschfristen für Daten	☒
	Definition und Dokumentation von Verfahren zur Entsorgung und Vernichtung von Datenträgen Dokumentation eines Löschkonzeptes für die Auftragsverarbeitung (SF Empfehlung A B C D)	☒
	Umsetzung von Regelungen zum Umgang mit elektr. Speichermedien	☐
	Umsetzung von Regelungen zur Entsorgung von Speichermedien	☐

Kommentiert [SG(12]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(13]: @GCSP/BW: Bitte Begründung angeben.

	Integritätskontrolle bei Löschungen bzw. Löschroutinen	☒
	Umgesetzte Löschung auf Entwicklungs-, Test- und Produktivumgebungen	☒
	Falls Sie andere oder zusätzliche Maßnahmen zum Löschen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollten Maßnahmen zur Löschung für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an:	
4. Belastbarkeit der Systeme und Dienste	*Belastbarkeit der Systeme u. Dienste beschreibt die Absicherung der Werte (hier: personenbezogene Daten) gegen ungewollten, zufälligen oder unrechtmäßigen Verlust oder Einschränkung (Störungen) von einem oder mehreren der klassischen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) sowie, dass Systeme und Dienste nach einer Störung in angemessener Zeit wieder in den Normalbetrieb überführt werden können. Im Falle einer Störung sollen deren Auswirkungen auf die drei vorherig beschriebenen klassischen Schutzziele möglichst gering sein.*	
4.1 Absicherung gegen Störungen (Kontinuitätssicherung)	*Loadbalancer*	☐
	Virenscanner mit aktuellen Suchmustern	☐
	Redundant ausgelegte IT-Systeme (SF Empfehlung A B C D)	☒
	Penetrationstests	☐
	Maßnahmen zur Steigerung der Aufrechterhaltung der Funktionalität von Systemen	☐
	Moderne Firewall Systeme	☐
	Ein RAID-System wird betrieben	☐
	Intrusion Detection Systeme (SF Empfehlung A B C D F)	☐
	Intrusion Prevention Systeme	☐

Kommentiert [SG(14]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(15]: @GCSP/BW: Bitte Begründung angeben.

	(SF Empfehlung D)	
	Divers ausgelegte Systeme	☐
	Maßnahmen zur Steigerung der Fehlertoleranz von Systemen und Diensten	☐
	Unverzügliche Wiederherstellung der Verfügbarkeit Bei Websites und Webanwendungen: Content-Security-Policy (CSP) ist definiert und umgesetzt	☐
	Falls Sie andere oder zusätzliche Maßnahmen zur Absicherung der Kontinuität der Systeme und Dienste umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollte die Absicherung der Kontinuität der Systeme und Dienste für die hier beauftragte Auftragsverarbeitung nicht relevant sein, geben Sie hier eine kurze Begründung dafür an:	
4.2 Wiederanlauf und Wiederherstellung der Verfügbarkeit	*Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)* *(SF Empfehlung A B C D)*	☒
	Dokumentiertes und getestetes Notfallkonzept	☐
	Dokumentiertes und getestetes IT-Service Continuity Management *(SF Empfehlung A B C D)*	☐
	Dokumentiertes und etabliertes Business Continuity Management *(SF Empfehlung A B C D)*	☐
	Dokumentiertes und etabliertes Disaster Recovery Management	☐
	Falls Sie andere oder zusätzliche Maßnahmen Steigerung der Wiederherstellbarkeit der Verfügbarkeit der Systeme und Dienste umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	

Kommentiert [SG(16]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(17]: @GCSP/BW: Bitte Begründung angeben.

	Sollten Maßnahmen zum Wiederanlauf und zur Wiederherstellung der Verfügbarkeit für die hier beauftragte Auftragsverarbeitung nicht relevant sein, geben Sie hier eine kurze Begründung dafür an:	
5. Organisatorische und Prozessuale Schutzmaßnahmen	*Durch organisatorische und prozessuale Schutzmaßnahmen werden die oben genannten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit nachhaltig abgesichert.*	
5.1 Organisatorische Sicherheitsmaßnahmen	*Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz*	☒
	Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit	☒
	Existenz eines angemessenen Informationssicherheitsmanagements	☒
	Existenz eines angemessenen Incident Managements (Reaktion auf Sicherheitsverletzungen) (SF Empfehlung A B C D)	☒
	Es existiert eine Angriffserkennung und Meldungsmöglichkeiten (Incident-Responce)	☒
	Schriftlich dokumentierter Change Management Prozess für IT-Systeme die personenbezogene Daten im Kontext diese Vertrages verarbeiten (SF Empfehlung A B C D)	☒
	Schriftlich dokumentierter und getesteter Patch Management Prozess für IT-Systeme die personenbezogene Daten im Kontext diese Vertrages verarbeiten	☒
	Informationen über technische Schwachstellen zu den genutzten Assets werden gesammelt und bewertet	☒
	Vorlage eines Sicherheitskonzepts nach behördlichen Mindestanforderungen (z.B. BSI)	☒
	Potenziell von technischen Schwachstellen betroffene Systemen und Software (Assets) werden	☒

Kommentiert [SG(18]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(19]: @GCSP/BW: Bitte Begründung angeben.

	identifiziert (z. B. Hersteller, Version, Installationsort)	
	Gewährleistung von Reaktionsmöglichkeiten bei technischen Schwachstellen:	☒
	Abtrennung der betroffenen Systeme	☒
	Abschalten des betroffenen Service	☒
	Anpassung von Zugriffsmöglichkeiten wie z. B. Firewalls	☒
	Anpassen des Monitorings	☒
	Erhöhung der Awareness der Anwender	☒
	Durchführung einer Informationsklassifizierung	☒
	In der Test- und Entwicklungsumgebung werden nur synthetische Daten, also keine Echtdaten oder personenbezogene Daten verarbeitet	☐
	Die Nutzung von mobilen Endgeräten (z. B. Smartphones, Notebooks) durch Mitarbeiter außerhalb der Liegenschaften und Büros ist geregelt	☐
	Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme	☐
	Prozess zur regelmäßigen Überprüfung der Wirksamkeit aller Schutzmaßnahmen und gegebenenfalls deren Anpassung zur Gewährleistung der Sicherheit der Verarbeitung (SF Empfehlung A B C D)	☐
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:	
	Sollten die organisatorischen Sicherheitskriterien für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an:	

Kommentiert [SG(20]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(21]: @GCSP/BW: Bitte Begründung angeben.

5.2 Auftragskontrolle	*Dokumentation aller Subunternehmer, die für die Verarbeitung der in diesem Vertrag beschriebenen personenbezogenen Daten eingesetzt werden*	☐
	Es erfolgen regelmäßige Subunternehmer-Audits	☐
	Dokumentierte Prozesse der gesamten Organisation liegen vor (SF Empfehlung A B C D F)	☐
	Es liegen historisierte und versionisierte SLAs und OLAs vor	☐
	Es existiert ein vollständiges Qualitäts-Management System bei den relevanten Subunternehmern	☐
	Es existiert ein vollständiges Informationssicherheits-Management System (ISMS) bei den relevanten Subunternehmern (SF Empfehlung A B C D F)	☐
	Alle eingesetzten relevanten Subunternehmer verfügen über eine Zertifizierung in Bereich Informationssicherheit, ausgestellt von einer akkreditierten Zertifizierungsstelle (z.B. IS27001, TISAX, SOC 2, BSI IT-Grundschutz)	☐
	Die regelmäßige Kontrolle der relevanten Subunternehmer erfolgt durch (SF Empfehlung A B C D F)	☐
	Vorlage von Self-Assessments	☐
	Vorlage von Assessments durch Dritte (z.B. Wirtschaftsprüfer, Behörden)	☐
	Vorlage der Verträge mit (weiteren) Subunternehmern	☐
	Durchführung von Kontrollen bei Subunternehmern	☐
	Vorhandensein von Richtlinien und Arbeitsanweisungen für die Verarbeitung im Auftrag	☒
	Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen	

	Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:
	Sollte die Auftragskontrolle für die hier beauftragte Dienstleistung nicht maßgeblich sein, geben Sie hier eine kurze Begründung dafür an: *Keine Subunternehmer*

Kommentiert [SG(22]: @GCSP/BW: Bitte befüllen

Kommentiert [SG(23]: @GCSP/BW: Bitte Begründung angeben.

Die folgenden technischen und organisatorischen Maßnahmen spiegeln die Maßnahmen wider, die in den einzelnen Funktionsbereichen der relevanten Umgebung umgesetzt werden. Je nach Unterfunktion und Anwendung sind möglicherweise nicht alle der nachfolgend genannten Maßnahmen vollständig umgesetzt (z. B. spezielle Maßnahmen zur Zugangskontrolle für Anwendungen, die bereits in besonders geschützten Umgebungen betrieben werden, wie z. B. besonders geschützte Rechenzentren). Spezifische Detailbeschreibungen der technischen und organisatorischen Maßnahmen für jede Produktkomponente, Unterfunktion oder (Teil-)Anwendung werden auf Anfrage zur Verfügung gestellt).

Für B2B Connect-bezogene Verarbeitungstätigkeiten (einschließlich Business Analytics und Kampagnen-/Marketingunterstützung) gelten die folgenden TOM:

1. Zugangssteuerung (physisch)	Ja	Nein	Nicht zutreffend
Die Bereiche mit Systemen, in denen Anwendungen personenbezogene Daten verarbeiten, sind in verschiedene Sicherheitszonen unterteilt	☒	☐	☐
Angabe der berechtigten Personen, einschließlich des Umfangs der Befugnisse in Bezug auf den physischen Zugang zu relevanten Räumen oder Bereichen	☒	☐	☐
Ausgestellte Zutrittsberechtigungsausweise	☒	☐	☐
Regeln und Vorschriften für Besucher sind vorhanden	☒	☐	☐
Regeln und Vorschriften für Schlüssel umgesetzt	☒	☐	☐
Alle Personen erfasst, die ein- und ausgehen	☒	☐	☐
Physischer Schutz des Firmengeländes (z. B. Zaun, Außenmauern, Kontrollpunkte)	☒	☐	☐
Sicherer Eingang (z. B. Schließsystem, ID-Leser)	☒	☐	☐
Einbruchhemmende Fenster	☒	☐	☐
Überwachungsanlage (z. B. Alarmanlage, Videoüberwachung)	☒	☐	☐
Trennsystem (z. B. Drehkreuze, Doppeltürsystem)	☒	☐	☐
Dokumentation der physischen Schutzmaßnahmen	☒	☐	☐

2. Zugangssteuerung (Systeme)	Ja	Nein	Nicht zutreffend
Dokumentiertes Sicherheitskonzept für den Zugang (Anmeldung) zur Anwendung	☒	☐	☐
Nutzung des Globalen Authentifizierungsdienstes (GAS)	☒	☐	☐
Regelmäßige Synchronisierung mit dem Unternehmensverzeichnis	☒	☐	☐
Verwendung des Secure Application Gateway (SAGW/WCP)	☐	☐	☒
Zugangsberechtigung angegeben und geprüft	☒	☐	☐
Benutzer identifiziert und Berechtigung überprüft	☒	☐	☐
System zur Verwaltung der Benutzeridentität implementiert	☒	☐	☐

Spezielle Authentifizierungsverfahren (z. B. Chipkarten, biometrische Zugangskontrolle)	☐	☐	☒
Angemessener Passwortschutz (verbindliche Vorgaben für sichere Passwörter, verschlüsselte Speicherung)	☒	☐	☐
Überwachung der Zugriffsversuche, einschließlich Reaktion auf Sicherheitsprobleme	☒	☐	☐
Isolierung des internen Netzes (z. B. durch VPN, Firewalls)	☒	☐	☐
Sofortige Löschung der Konten ehemaliger Mitarbeiter	☐	☒	☐
Spezielle Sicherheitssoftware (z. B. Anti-Malware, Intrusion Detection)	☒	☐	☐
Regeln und Vorschriften für Besucher sind vorhanden	☒	☐	☐
Regeln und Vorschriften für den Fernzugriff	☒	☐	☐

3. Zugangssteuerung (Benutzerrechte)	Ja	Nein	Nicht zutreffend
Berechtigungs- und Rollenkonzept für Anwendungen implementiert	☒	☐	☐
Für den Datenzugriff erforderliche Benutzerkonten	☒	☐	☐
Regelmäßige Überprüfung der Berechtigungen	☐	☒	☐
Auferlegte Zugangsbeschränkungen (basierend auf den Prinzipien der Erforderlichkeit und der geringsten Berechtigung)	☒	☐	☐
Zusätzliche Passwörter (basierend auf dem 4-Augen-Prinzip) für besonders wichtige Funktionen (z. B. Systemadmin)	☒	☐	☐
Sicherstellung der Mehrmandantenfähigkeit des Systems	☒	☐	☐
Getrennte und mehrmandantenfähige Datenbanken	☒	☐	☐
Trennung von Entwicklungs-, Test-, Integrations- und Produktionsumgebung	☒	☐	☐
Trennung von Produktivumgebung und Archivierung	☒	☐	☐
Lesezugriff protokolliert	☒	☐	☐
Schreibzugriff protokolliert	☒	☐	☐
Unerlaubte Zugriffsversuche protokolliert	☒	☐	☐
Implementierung von Aufbewahrungsfristen für Daten	☒	☐	☐

4. Offenlegungskontrolle	Ja	Nein	Nicht zutreffend
Datenübertragung verschlüsselt	☒	☐	☐
Datenspeicherung verschlüsselt	☐	☒	☐
Mobile Endgeräte verschlüsselt (z. B. Festplattenverschlüsselung)	☐	☐	☒
Datenweiterleitung oder -übertragung protokolliert	☒	☐	☐
Formen der Datenweitergabe vollständig dokumentiert (z. B. Ausdruck, Datenträger, automatisierte Übertragung)	☐	☐	☒
Schnittstellen dokumentiert	☒	☐	☐
Einschränkung der Rechte bei der Datenübermittlung	☒	☐	☐
Plausibilitäts-, Vollständigkeits- und Genauigkeitsprüfungen der Daten durchgeführt	☒	☐	☐
Deaktivierung der USB-Schnittstelle	☐	☐	☒
Vorschriften zum Umgang mit mobilen Geräten umgesetzt	☐	☐	☒
Vorschriften zur Entsorgung von Datenträgern umgesetzt	☒	☐	☐
Schutz vor Datenmanipulation (Malware-Schutz)	☒	☐	☐

5. Eingabekontrolle	Ja	Nein	Nicht zutreffend
Systemprotokollierung/Aufzeichnung sichergestellt	☒	☐	☐
Regelmäßige Auswertung von Logfiles/Protokollen	☐	☒	☐
Gewährleistung der Aufgabentrennung (SoD) (SoD-Matrix definiert und Verfahren implementiert)	☒	☐	☐
Berechtigung zur Eingabe, Änderung oder Löschung von Daten dokumentiert	☒	☐	☐
Eingabe/Änderung von Daten vollständig protokolliert/aufgezeichnet	☐	☐	☒
Eingabe/Änderung von teilweise protokollierten/aufgezeichneten Daten	☒	☐	☐
Änderung/Löschung von Daten verboten	☒	☐	☐
Elektronische Unterschrift zur Sicherstellung der Authentizität von Datenveränderungen	☐	☐	☒

6. Auftragskontrolle	Ja	Nein	Nicht zutreffend
Die Mercedes-Benz-Standardvereinbarung zur Auftragsdatenverarbeitung wurde vereinbart	☒	☐	☐
Die Standardvereinbarung des Datenverarbeiters über die Auftragsdatenverarbeitung wurde vereinbart	☒	☐	☐
Für die Datenverarbeitung durch Auftragsverarbeiter in Drittländern wurden die Standardvertragsklauseln der EU-Kommission vereinbart	☒	☐	☐
Die Zuständigkeiten des für die Datenverarbeitung Verantwortlichen und des Datenverarbeiters sind streng geregelt/getrennt	☒	☐	☐
Regeln zur Anpassung/Änderung von Anweisungen an den Datenverarbeiter	☒	☐	☐
Der für die Datenverarbeitung Verantwortliche hat Kontrollen vor Ort durchgeführt und dokumentiert	☐	☒	☐
Der Datenverarbeiter hat Selbstbeurteilungen vorgelegt	☐	☒	☐
Der Datenverarbeiter hat genehmigte Bescheinigungen vorgelegt	☐	☒	☐
Der Datenverarbeiter hat eine Liste von Unterauftragsverarbeitern vorgelegt	☒	☐	☐
Kontrollen von Unterauftragsverarbeitern durch den Verarbeiter	☐	☒	☐

7. Verfügbarkeitskontrolle	Ja	Nein	Nicht zutreffend
Regelmäßige Überprüfung des Systemzustands (Überwachung)	☒	☐	☐
Sicherungs- und Wiederherstellungsplan (regelmäßige Datensicherungen)	☒	☐	☐
Strategie zur Datenarchivierung umgesetzt	☒	☐	☐
Dokumentierte Notfallpläne (Business Continuity, Disaster Recovery)	☒	☐	☐
Regelmäßig getestete Notfallpläne	☐	☒	☐
Vorhandensein von redundanten IT-Systemen (Server, Speicher usw.) bewertet	☒	☐	☐
Voll funktionsfähige physische Schutzsysteme vorhanden (Brandschutz, Energie, Klimaanlage)	☒	☐	☐

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen	**Ja**	**Nein**	**Nicht zutreffend**
Regelmäßige Überprüfung des Systemzustands (Monitoring)	☒	☐	☐
Überprüfung der Umsetzung der beschriebenen Maßnahmen	☒	☐	☐
Beschreibung der geltenden Datenschutzanforderungen in verbindlichen Richtlinien und Handlungsanweisungen	☒	☐	☐
Einbindung des Datenschutzbeauftragten in relevante neue Datenverarbeitungsprozesse	☒	☐	☐

Für Verarbeitungstätigkeiten im Zusammenhang mit WebParts (einschließlich Business Analytics und Unterstützung von Kampagnen/Marketing) gelten die folgenden TOM:

1. Zugangssteuerung (physisch)	Ja	Nein	Nicht zutreffend
Die Bereiche mit Systemen, in denen Anwendungen personenbezogene Daten verarbeiten, sind in verschiedene Sicherheitszonen unterteilt	☒	☐	☐
Angabe der berechtigten Personen, einschließlich des Umfangs der Befugnisse in Bezug auf den physischen Zugang zu relevanten Räumen oder Bereichen	☒	☐	☐
Ausgestellte Zutrittsberechtigungsausweise	☒	☐	☐
Regeln und Vorschriften für Besucher sind vorhanden	☒	☐	☐
Regeln und Vorschriften für Schlüssel umgesetzt	☒	☐	☐
Alle Personen erfasst, die ein- und ausgehen	☒	☐	☐
Physischer Schutz des Firmengeländes (z. B. Zaun, Außenmauern, Kontrollpunkte)	☒	☐	☐
Sicherer Eingang (z. B. Schließsystem, ID-Leser)	☒	☐	☐
Einbruchhemmende Fenster	☐	☐	☒
Überwachungsanlage (z. B. Alarmanlage, Videoüberwachung)	☒	☐	☐
Trennsystem (z. B. Drehkreuze, Doppeltürsystem)	☒	☐	☐
Dokumentation der physischen Schutzmaßnahmen	☒	☐	☐

2. Zugangssteuerung (Systeme)	Ja	Nein	Nicht zutreffend
Dokumentiertes Sicherheitskonzept für den Zugang (Anmeldung) zur Anwendung	☐	☒	☐
Nutzung des Globalen Authentifizierungsdienstes (GAS)	☒	☐	☐
Regelmäßige Synchronisierung mit dem Unternehmensverzeichnis	☒	☐	☐
Verwendung des Secure Application Gateway (SAGW/WCP)	☒	☐	☐
Zugangsberechtigung angegeben und geprüft	☒	☐	☐
Benutzer identifiziert und Berechtigung überprüft	☒	☐	☐
System zur Verwaltung der Benutzeridentität implementiert	☒	☐	☐
Spezielle Authentifizierungsverfahren (z. B. Chipkarten, biometrische Zugangskontrolle)	☐	☒	☐
Angemessener Passwortschutz (verbindliche Vorgaben für sichere Passwörter, verschlüsselte Speicherung)	☒	☐	☐
Überwachung der Zugriffsversuche, einschließlich Reaktion auf Sicherheitsprobleme	☒	☐	☐
Isolierung des internen Netzes (z. B. durch VPN, Firewalls)	☒	☐	☐
Sofortige Löschung der Konten ehemaliger Mitarbeiter	☒	☐	☐
Spezielle Sicherheitssoftware (z. B. Anti-Malware, Intrusion Detection)	☒	☐	☐
Regeln und Vorschriften für Besucher sind vorhanden	☒	☐	☐
Regeln und Vorschriften für den Fernzugriff	☒	☐	☐

3. Zugangssteuerung (Benutzerrechte)	Ja	Nein	Nicht zutreffend
Berechtigungs- und Rollenkonzept für Anwendungen implementiert	☒	☐	☐
Für den Datenzugriff erforderliche Benutzerkonten	☒	☐	☐
Regelmäßige Überprüfung der Berechtigungen	☒	☐	☐
Auferlegte Zugangsbeschränkungen (basierend auf den Prinzipien der Erforderlichkeit und der geringsten Berechtigung)	☒	☐	☐

Zusätzliche Passwörter (basierend auf dem 4-Augen-Prinzip) für besonders wichtige Funktionen (z. B. Systemadmin)	☐	☒	☐
Sicherstellung der Mehrmandantenfähigkeit des Systems	☒	☐	☐
Getrennte und mehrmandantenfähige Datenbanken	☐	☒	☐
Trennung von Entwicklungs-, Test-, Integrations- und Produktionsumgebung	☒	☐	☐
Trennung von Produktivumgebung und Archivierung	☒	☐	☐
Lesezugriff protokolliert	☒	☐	☐
Schreibzugriff protokolliert	☒	☐	☐
Unerlaubte Zugriffsversuche protokolliert	☐	☐	☒
Implementierung von Aufbewahrungsfristen für Daten	☐	☒	☐

4. Offenlegungskontrolle	Ja	Nein	Nicht zutreffend
Datenübertragung verschlüsselt	☒	☐	☐
Datenspeicherung verschlüsselt	☒	☐	☐
Mobile Endgeräte verschlüsselt (z. B. Festplattenverschlüsselung)	☐	☐	☒
Datenweiterleitung oder -übertragung protokolliert	☒	☐	☐
Formen der Datenweitergabe vollständig dokumentiert (z. B. Ausdruck, Datenträger, automatisierte Übertragung)	☒	☐	☐
Schnittstellen dokumentiert	☒	☐	☐
Einschränkung der Rechte bei der Datenübermittlung	☒	☐	☐
Plausibilitäts-, Vollständigkeits- und Genauigkeitsprüfungen der Daten durchgeführt	☒	☐	☐
Deaktivierung der USB-Schnittstelle	☐	☐	☒
Vorschriften zum Umgang mit mobilen Geräten umgesetzt	☐	☐	☒
Vorschriften zur Entsorgung von Datenträgern umgesetzt	☐	☐	☒
Schutz vor Datenmanipulation (Malware-Schutz)	☐	☐	☒

5. Eingabekontrolle	Ja	Nein	Nicht zutreffend
Systemprotokollierung/Aufzeichnung sichergestellt	☒	☐	☐
Regelmäßige Auswertung von Logfiles/Protokollen	☒	☐	☐
Gewährleistung der Aufgabentrennung (SoD) (SoD-Matrix definiert und Verfahren implementiert)	☒	☐	☐
Berechtigung zur Eingabe, Änderung oder Löschung von Daten dokumentiert	☐	☐	☒
Eingabe/Änderung von Daten vollständig protokolliert/aufgezeichnet	☐	☒	☐
Eingabe/Änderung von teilweise protokollierten/aufgezeichneten Daten	☒	☐	☐
Änderung/Löschung von Daten verboten	☐	☐	☒
Elektronische Unterschrift zur Sicherstellung der Authentizität von Datenveränderungen	☐	☒	☐

6. Auftragskontrolle	Ja	Nein	Nicht zutreffend
Die Mercedes-Benz-Standardvereinbarung zur Auftragsdatenverarbeitung wurde vereinbart	☐	☒	☐
Die Standardvereinbarung des Datenverarbeiters über die Auftragsdatenverarbeitung wurde vereinbart	☐	☒	☐
Für die Datenverarbeitung durch Auftragsverarbeiter in Drittländern wurden die Standardvertragsklauseln der EU-Kommission vereinbart	☐	☒	☐

Die Zuständigkeiten des für die Datenverarbeitung Verantwortlichen und des Datenverarbeiters sind streng geregelt/getrennt	☒	☐	☐
Regeln zur Anpassung/Änderung von Anweisungen an den Datenverarbeiter	☒	☐	☐
Der für die Datenverarbeitung Verantwortliche hat Kontrollen vor Ort durchgeführt und dokumentiert	☐	☒	☐
Der Datenverarbeiter hat Selbstbeurteilungen vorgelegt	☐	☒	☐
Der Datenverarbeiter hat genehmigte Bescheinigungen vorgelegt	☐	☒	☐
Der Datenverarbeiter hat eine Liste von Unterauftragsverarbeitern vorgelegt	☒	☐	☐
Kontrollen von Unterauftragsverarbeitern durch den Verarbeiter	☐	☐	☒

7. Verfügbarkeitskontrolle	Ja	Nein	Nicht zutreffend
Regelmäßige Überprüfung des Systemzustands (Überwachung)	☒	☐	☐
Sicherungs- und Wiederherstellungsplan (regelmäßige Datensicherungen)	☒	☐	☐
Strategie zur Datenarchivierung umgesetzt	☒	☐	☐
Dokumentierte Notfallpläne (Business Continuity, Disaster Recovery)	☒	☐	☐
Regelmäßig getestete Notfallpläne	☐	☒	☐
Vorhandensein von redundanten IT-Systemen (Server, Speicher usw.) bewertet	☒	☐	☐
Voll funktionsfähige physische Schutzsysteme vorhanden (Brandschutz, Energie, Klimaanlage)	☒	☐	☐

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen	**Ja**	**Nein**	**Nicht zutreffend**
Regelmäßige Überprüfung des Systemzustands (Monitoring)	☒	☐	☐
Überprüfung der Umsetzung der beschriebenen Maßnahmen	☒	☐	☐
Beschreibung der geltenden Datenschutzanforderungen in verbindlichen Richtlinien und Handlungsanweisungen	☒	☐	☐
Einbindung des Datenschutzbeauftragten in relevante neue Datenverarbeitungsprozesse	☒	☐	☐

B2B Connect – nur für den internen Gebrauch – Entwurf
Überprüfung durch den örtlichen Rechtsbeistand erforderlich

Anhang 3: Unterauftragsverarbeiter

#	*Unterauftragsverarbeiter für Mercedes-Benz AG einschließlich Adresse / Standort*	*Gegenstand und Art der Verarbeitung*	*Laufzeit*

Anhang 2: Plattformregeln

1. Allgemeine Plattformregeln

Mercedes-Benz AG behält sich das Recht vor, Partner oder Kunden (im Folgenden zusammen "Nutzer" genannt) bei Anzeichen einer missbräuchlichen Nutzung von B2B Connect oder einer Nutzung, die gegen die geltenden Vertragsbestimmungen verstößt, zu sperren oder andere angemessene Maßnahmen zu ergreifen. Die Nutzung gilt insbesondere dann als missbräuchlich, wenn der Nutzer B2B Connect oder darüber bereitgestellte Informationen für andere als die vorgesehenen Zwecke, für illegale oder gegen die Rechte von Mercedes-Benz AG oder Dritten verstoßende Zwecke oder unter Verletzung mit sonstigen Richtlinien von Mercedes-Benz AG verwendet.

Kommentiert [HB(24]: MBAG, überall anpassen

Der Nutzer sichert zu, dass sämtliche Mercedes-Benz AG und anderen Nutzern bereitgestellten Informationen jederzeit wahr, genau und vollständig sind und alle gesetzlichen Anforderungen und geltenden Vertragsbestimmungen erfüllen. Der Nutzer verpflichtet sich, Mercedes-Benz AG unverzüglich über künftige wesentliche Änderungen der Mercedes-Benz AG bereitgestellten Informationen, die für das Vertrags- oder Nutzungsverhältnis relevant sind, in Kenntnis zu setzen.

Es ist insbesondere nicht gestattet, B2B Connect zur Verbreitung von Informationen zu nutzen, die folgende Kriterien erfüllen: rassistische, menschenverachtende Slogans; falsche oder anderweitig nicht richtige Informationen; Informationen, die anstößig, beleidigend, belästigend, gehässig, obszön, bedrohlich oder anderweitig verwerflich sind; Informationen, die gegen gesetzliche Anforderungen verstoßen oder geltende Anforderungen nicht hinreichend einhalten oder umsetzen (z. B. im Falle von Kennzeichnungs- oder Transparenzpflichten); Informationen, deren Bereitstellung oder Verbreitung eine Straftat bzw. ein Vergehen begründet; Informationen, deren Bereitstellung oder Verbreitung eine Straftat bzw. eine Ordnungswidrigkeit begründet.

Sofern die bereitgestellten Informationen gegen die geltenden Nutzungsbedingungen von B2B Connect verstoßen und Mercedes-Benz AG Kenntnis darüber erlangt (z. B. durch eine Meldung eines Kunden oder sonstigen Dritten), behält sich Mercedes-Benz AG das Recht vor, die entsprechenden Inhalte unverzüglich (falls nötig auch nur vorübergehend) zu sperren oder zu löschen und alle weiteren erforderlichen Maßnahmen zu ergreifen.

Sofern erforderlich oder angemessen, werden je nach Schwere, Häufigkeit und Anzahl der Verstöße die folgenden Maßnahmen ergriffen:

- vorübergehende oder dauerhafte Löschung von Inhalten;
- vorübergehende Sperrung eines Nutzerkontos oder Nutzerzugangs;
- Deaktivierung des Nutzerkontos oder Nutzerzugangs für drei Monate;
- dauerhafte Sperrung des Nutzerkontos und aller verbundenen Inhalte;
- Sperrung des Nutzerkontos und aller verbundenen Inhalte sowie Aufnahme der Zugangsdaten, insbesondere der angegebenen E-Mail-Adresse und anderer Stammdaten zur Identifikation des Nutzers, in eine Blacklist mit der Folge, dass kein neues Nutzerkonto und keine neuen Inhalte erstellt werden können;

Soweit gesetzlich zulässig wird der Nutzer über die Entscheidung von Mercedes-Benz AG in Kenntnis gesetzt und er erhält die Möglichkeit, darauf zu reagieren. Nach einer weiteren Reaktion (oder in Ermangelung einer solchen Reaktion) wird Mercedes-Benz AG die Entscheidung noch einmal prüfen und dann abschließend über den Umgang mit den betroffenen Inhalten entscheiden. Je nach Fall kommen, wie in den einschlägigen Nutzungsbedingungen von B2B Connect beschrieben, zusätzliche Moderationsmaßnahmen zur Anwendung. Der Nutzer erhält eine Mitteilung/E-Mail über die beschlossenen Moderationsmaßnahmen, einschließlich einer Begründung.

Anmerkungen und Anträge im Hinblick auf gemäß dem Gesetz über digitale Dienste beschlossene Moderationsmaßnahmen können an die in Abschnitt 3.2 aufgeführten Ansprechpartner gerichtet werden. Der Nutzer muss angeben, auf welche Entscheidung er sich bezieht (z. B. durch Angabe des Datums, Sachverhalts und/oder Aktenzeichens), inwieweit er Einwände hat oder im Hinblick worauf er genauerer Erklärung bedarf.

Beschwerden, die sich nicht über vorstehend beschriebene Prozesse beilegen lassen, können über eine anerkannte Schlichtungsstelle geklärt werden. Sofern erforderlich, werden Informationen zum Zugang zu einer solchen Schlichtungsstelle auf der B2B-Website unter "Rechtliche Hinweise" veröffentlicht. Ungeachtet der Einbindung einer solchen Stelle steht jederzeit der Rechtsweg offen.

2. Identifikation von geschäftlichen und werblichen Inhalten

Wenn Nutzer anderen Nutzern über B2B Connect Informationen bereitstellen, müssen geschäftliche Angebote und Werbung entsprechend den anwendbaren Gesetzen als solche erkennbar sein.

Im Zusammenhang mit Werbeangeboten müssen Nutzer auf transparente Weise über den Werbetreibenden informieren. Dies beinhaltet beispielsweise auch, in wessen Namen die Werbung angezeigt wird und wer für die Werbeanzeige bezahlt hat.

Werden Werbeanzeigen unterschiedlichen Nutzern oder Nutzergruppen angezeigt – je nach deren Verhalten oder dergleichen (insbesondere im Falle von Targeting oder Profiling) –, muss der Nutzer auf transparente Weise über die relevanten Parameter informieren, anhand derer bestimmt wird, welche Informationen welchen Nutzern oder Nutzergruppen angezeigt werden. Nutzer müssen sämtliche Informationen jederzeit auf dem neuesten Stand halten.

Mercedes-Benz AG wird in B2B Connect möglichst technische Mittel und Optionen bereitstellen, in deren Rahmen der Nutzer seinen entsprechenden Pflichten nachkommen kann. Sollten keine solchen Mittel bereitgestellt werden oder sollten die Mittel aus Sicht des Nutzers nicht ausreichend sein, muss er Mercedes-Benz AG unverzüglich darüber in Kenntnis setzen und die Parteien werden umgehend die Einführung entsprechender Mittel regeln.

3. Ansprechpartner

Bei Fragen zu B2B Connect kann der Nutzer sich an die Ansprechpartner wenden, die auf der B2B-Website unter "Anbieter / Datenschutz" aufgeführt sind. Bei der Kontaktaufnahme zu Mercedes-Benz AG sollte der Nutzer sein Anliegen stets spezifizieren, indem er angibt, worauf sich sein Anliegen bezieht, aus welchen Gründen er in diesem Zusammenhang Kontakt zu Mercedes-Benz AG aufnimmt und wie Mercedes-Benz AG den Nutzer diesbezüglich unterstützen kann.

3.1 Illegale Inhalte

Wenn der Nutzer illegale Inhalte oder Verstöße gegen die geltenden Nutzungsbedingungen von B2B Connect melden möchte, kann er das auf der B2B-Website unter "Anbieter / Datenschutz" bereitgestellte Kontaktformular verwenden. Bei der Kontaktaufnahme zu Mercedes-Benz AG sollte der Nutzer sein Anliegen stets spezifizieren, indem er beispielsweise angibt, warum er glaubt, dass bestimmte Inhalte illegal sind oder gegen bestimmte Regelungen verstoßen, wo entsprechende Inhalte zu finden sind, wann der Nutzer darauf gestoßen ist usw.

3.2 Beschwerden und Fragen im Zusammenhang mit einer Entscheidung

Wenn der Nutzer sich mit einer Beschwerde bezüglich einer gegen ihn getroffenen Entscheidung, wie vorstehend beschrieben, an Mercedes-Benz AG wenden möchte, sollte der Nutzer das auf der B2B-Website unter "Anbieter / Datenschutz" bereitgestellte Kontaktformular verwenden.

***