

## Mercedes-Benz-internal use only-draft Review by local legal counsel required

### Terms of Use for authorized service partners for B2B Connect Seller Center and WebParts Dealer Client

between *Silver Star Motors EAD* Bulgaria, 1839 Sofia, 52 Chelopesko shose str. (name and address) (hereinafter referred to as "Silver Star Motors EAD") and the authorized service partner (name and address) (hereinafter referred to as "**Partner**") of *Silver Star Motors EAD* participating in B2B Connect and related services (B2B Connect Seller Center and WebParts Dealer Client) are hereafter referred to collectively as "**B2B Connect**".

Customers in this context are Business to Business independent entrepreneurs conducting automotive repair and maintenance services (such as individual service providers and fleet customers) (hereinafter also referred to as "**Customer**").

Silver Star Motors EAD and Partner are hereinafter also referred to as "**Parties**".

#### Preamble

B2B Connect is provided by Silver Star Motors EAD. B2B Connect is a technical ecosystem which integrates Mercedes-Benz genuine parts sales via B2B Connect Seller Center (as available in the Mercedes-Benz Aftersales ecosystem) as well as repair and maintenance solutions, as far as available in the relevant market, offered to Customers by other subsystems. For Partners services around B2B Connect are offered via WebParts Dealer Client and B2B Connect Seller Center. Features from WebParts Dealer Client will be subsequently migrated to B2B Connect Seller Center.

The Customer receives access to B2B Connect by self-registration and can customize its data, while the online ordering of Mercedes-Benz genuine parts via B2B Connect is only available for the Customer after the acceptance and activation by the Partner in WebParts Dealer Client (also after migration by B2B Connect Seller Center).

The aim of the current WebParts Dealer Client and B2B Connect Seller Center is to provide the Partner a customer-oriented, systemic solution on the internet, as a marketing tool in After-Sales (over-the-counter business) as well as the increase of competitiveness and profitability in the After-Sales business. The provisions of the Authorized Service Agreement also apply to these Terms of Use.

The Customer data for the ordering process is displayed to the Partner via WebParts Dealer Client and in future via B2B Connect Seller Center and can be imported to the Partner's management system.

#### § 1 System requirements

To display the parts availability of the Partner to the Customer, the Partner must be connected to the Logistikbus, which is being provided by Silver Star Motors EAD in cooperation with MBAG. Otherwise, there is a limited availability of information.

#### § 2 Silver Star Motors EAD Services, Conclusion of contracts, Change, Participation and 5\*Rater

Silver Star Motors EAD provides the Partner B2B Connect Seller Center and WebParts Dealer Client that enable the online ordering of genuine parts for Customers of the Partner.

By Silver Star Motors EAD provided B2B Connect Seller Center and WebParts Dealer Client enables the Partner to:

- see the activated Customers,
- adjust list prices,
- define discount rates,
- define own Customer discount codes,
- assign the selected Customer discount code,
- define own discount groups,
- define information regarding estimated time of arrival

- support of Customer requests
- receive feedback of its products, services and overall performance from Customers via the 5\*Rater,
- receive customized campaign proposals and campaign support services based on information related to transactions executed via B2B Connect with Customers (i.e. customer name, order related information etc.)
- manage order requests and Customer transactions from B2B Connect and PartsLink24

When participating in B2B Connect Customers can rate the products, services and overall performance of Partner through the 5\*Rater. With participating and making use of B2B Connect Seller Center and WebParts Dealer Client Partner acknowledges and accepts the fact that Customer feedback is provided and that Silver Star Motors EAD will receive this information in an aggregated form (not containing any information related to particular transactions) and shall be entitled to use this information for market and Partner performance reviews and steering of the overall performance and collaboration with Partner. Further details with regards to the use of personal data in this context are set out in **Appendix 1** to these Terms of Use.

Based on the data entered by the Customer, the Customer can order via the Internet from the Partner, whereby the Customer-specific price and the availability for the respective Mercedes-Benz genuine part are displayed. The prerequisite for this is that Customer has registered for B2B Connect and activation of the Customer by the Partner in WebParts Dealer Client. The Customer order is transferred to the Partner via B2B Connect. It can be read out by the Partner via a standard export format and can be imported into the Partner's managementsystem.

The Partner shall be free to select whether to accept orders, and which of the orders received it wishes to accept. Where the Partner and a Customer have not made any agreement to the contrary, a contract shall be deemed formed at such time as the Partner accepts the order of a Customer by forwarding an order acceptance. The performance of contracts made via B2B Connect is a matter lying within the sole responsibility of the respective Partner. With respect to contracts managed via B2B Connect, Silver Star Motors EAD neither assumes any warranty for performance of contracts made between Partner and Customers via B2B Connect. Silver Star Motors EAD shall bear no duty whatsoever to ensure performance of the contracts which have been formed between Partner and Customers.

Silver Star Motors EAD is entitled to change the functions provided through B2B Connect if such a change would not require a change to these Terms of Use. Silver Star Motors EAD shall notify Partner in textual form (e.g. email) at least one month prior to such change unless otherwise agreed.

Unless otherwise agreed Silver Star Motors EAD shall be entitled to amend these Terms of Use to the extent such a change is neutral or beneficial to Partner unilaterally at any time. Otherwise, Silver Star Motors EAD shall notify Partner in textual form at least six (6) weeks prior to such a change. If Partner does not object to such changes in textual form within four (4) weeks after having received such a notification the proposed changes shall become binding upon the parties six (6) weeks after the notification. Silver Star Motors EAD shall notify the Partner of the effect of not objecting to such changes together with such a notification. Partner shall have the right to object to such changes. If Partner objects, Silver Star Motors EAD shall have the right to terminate the Partner's use of the services affected by such a change for cause.

In case that Silver Star Motors EAD will integrate WebParts Dealer Client directly into B2B Connect Seller Center these Terms of Use shall continue to apply, subject to any necessary amendments to these Terms of Use that may be implemented in this context in accordance with the above regulations.

#### § 3 Use of B2B Connect Seller Center and WebParts Dealer Client

The Partner receives interested Customers - which he can activate

## Mercedes-Benz-internal use only-draft Review by local legal counsel required

for online ordering - via WebParts Dealer Client. The activation should take place without undue delay.

It is the responsibility of the Partner to ensure compliance with the contractual sales restrictions (in particular Authorized Service Agreement and Standards).

The master data, e.g. definition of discount rates for self-defined Customer discount classes, assignment of Mercedes-Benz genuine parts to self-defined discount groups or campaigns etc. must be entered into the system by the Partner.

The Partner is free in his pricing, granting of discounts and labeling Customer discounts. The prices, discounts, Customer discount codes or campaigns stored in the system or entered by the Partner, are displayed to the Customer when he sets the order, ensuring that the data is up to date is the responsibility of the Partner.

The Partner is obliged to place his general terms and conditions as well as his data protection regulations for his Customers in WebParts Dealer Client (and to obtain the respective acceptance to the extent necessary). The general terms and conditions of the Partner must set out sufficiently clear that the Partner is the seller of the genuine parts. The data protection regulations must set out sufficiently clear that the Partner is controller with regard to his Customers' data in relation to the conduct of an order. Further, the data protection regulations of the Partner must observe the respectively applicable data protection laws (including any information obligations), particularly those of the General Data Protection Regulation (GDPR). If at any time during the term of these Terms of Use, the Partner cannot offer the genuine parts in compliance with applicable data privacy laws, then Partner shall notify Silver Star Motors EAD. Partner shall have the option to propose a cure within a reasonable period of time required by Silver Star Motors EAD. If a solution proposed by Partner is not reasonably acceptable for Silver Star Motors EAD, Silver Star Motors EAD shall have the right to terminate these Terms of Use in whole or in part with immediate effect.

The objective of B2B Connect is the online presentation of the Partner's offers with regards to genuine parts. Customers are only allowed to use B2B Connect for this purpose.

The use of B2B Connect does not confer any rights on B2B Connect, the used URLs or the accompanying documentations (manual, Guided Tour, etc.), other than the right to use in accordance with these Terms of Use.

Partner undertakes to ensure that the hardware and software employed by him in the use of B2B Connect Seller Center and WebParts Dealer Client, to the extent applicable, including workstation computers, tablets, routers, data communication systems and so forth are free from any viruses, worms, Trojan horses, etc. With regard to any data uploaded by the Partner, Partner undertakes to ensure that he is the holder of all rights in the uploaded data and may freely dispose over their use, including that such uploaded data is not encumbered with third-party rights, which stand opposed to such a use.

Partner may support Customers through the B2B Connect Seller Center with complaints directed to Silver Star Motors EAD or other requests concerning B2B Connect upon request of the Customer. Such a support shall occur free of charge (no right to claim for compensation or reimbursement of costs or expenses against Silver Star Motors EAD and shall be solely provided in Partner's own responsibility and relationship towards Customer and without Silver Star Motors EAD assuming any responsibility for Partner's use of B2B Connect Seller Center or additional support provided to Customers. This shall also apply to the provision of any other transaction related information as provided by Partner to Customers (e.g. information on estimated time of arrival) in WebParts Dealer Client.

### **§ 4 Data Flow**

The Customer enters his data via self-registration on B2B Connect. This data is authenticated and stored by the provider Silver Star Motors EAD

The data are also provided to the Partner in B2B Connect Seller Center.

### **§ 5 Confidentiality**

The Parties shall treat as confidential all technical and economic information, including usage data by Customers, which will be directly or indirectly accessible to them during the term of these Terms of Use in connection with the use of B2B Connect. These data shall only be made accessible to third parties by Silver Star Motors EAD if this is necessary for the contractual fulfillment or otherwise provided for herein and if there is a corresponding confidentiality agreement in place with such third parties. Data about Customers activated by the Partner or Customer usage data will only be used by Silver Star Motors EAD for the performance of these Terms of Use and will be anonymized by Mercedes-Benz AG for the development of the platform.

## Mercedes-Benz-internal use only-draft Review by local legal counsel required

Information and documents that are not classified as confidential information are

- generally known information or information that come to be known without infringement of the obligations contained in these Terms of Use,
- Information that a Party verifiably created or won as part of its own work, or
- Information that Silver Star Motors EAD verifiably received legally from third parties.

A Party is exempt from the obligation to treat information confidentially if that Party has to disclose the information due to legal regulations or dispositions of the competent authorities.

### § 6 Data Protection

With respect to the selling and selling process regarding genuine parts/services via B2B Connect, the Parties intend to exchange the relevant personal data among independent controllers, whereas Silver Star Motors EAD shall be controller of the processing of personal data for the purpose of operating B2B Connect. Unless and until otherwise stipulated, the Parties generally do not intend to establish a joint controllership with regard to their individual processing of the Customer's personal data. To the extent the relationship between Silver Star Motors EAD Mercedes-Benz AG (and/or its affiliates) and/or Partner qualifies or is qualified as a joint controllership pursuant to Art. 26 of the (GDPR), the Parties will or agree to enter in the future into appropriate joint controllership agreements with the respective joint controller(s) stipulating the respective responsibilities of the joint controllers in accordance with Art. 26 GDPR.

Having said that, Silver Star Motors EAD processes personal data of Partner and Partner's Customers (i) on behalf of Partner as processor, and (ii) when using personal data in the 5\*Rate, for support through B2B Connect Seller Center, or for Business analytics and Marketing Campaign Services as Controller. The provisions on data protection agreed between the Parties are set forth in **Appendix 1** to these Terms of Use.

### § 7 Data quality, Partner's obligations

The Partner is responsible to keep the necessary information required for the offering/displaying of the genuine parts via WebParts Dealer Client (prices, discounts, availability, delivery times, etc.) up to date.

The Partner will regularly check online or after notification by electronic means whether an order of genuine parts has been made by Customers. The Partner will export these orders to the dealer management system and continue to process them. The Partner will process the orders within an adequate time and inform the Customer about the status of the order. An order confirmation to the Customer as to whether the delivery deadlines requested by the Customer can be complied with must be carried out on the conventional way.

Silver Star Motors EAD provides a suitable access protection system and, upon request, assigns access authorization to the Partner. The Partner undertakes to ensure the proper use of the system by his employees, including the use of proper applications when accessing the system. The Partner undertakes not to disclose the access authorization assigned to him to any unauthorized person. The Partner undertakes to respond to incoming registration acceptance requests of Customers within an adequate time and to provide in coordination with Silver Star Motors EAD 1st and 2nd level support for WebParts Dealer Client. Silver Star Motors EAD excludes any liability for the misuse of user ID and password in the Partner's organizational unit and his customers.

Silver Star Motors EAD reserves the right to block the user concerned in the event of signs of improper use. The Partner is informed directly of this.

B2B Connect is a technical solutions available worldwide. The Partner is responsible for regularly checking the applicable legal framework conditions in his country with regard to selling and selling process regarding genuine parts on B2B Connect, while Silver Star Motors EAD remains responsible for regularly checking the applicable legal framework conditions for the operation of B2B Connect.

Partner must in particular ensure that all requirements (including any necessary consents and information) are met in relation to Customers in order to provide the services regulated in these Terms of Use.

### § 8 Availability

Due to the present state of technology, the provision and use of B2B Connect may also be subject to certain restrictions and inaccuracies beyond the control of Silver Star Motors EAD. This applies in particular to the availability of internet access. Disruptions may also be caused by force majeure, including strikes, lockouts, or orders by the authorities, or result from technical or other measures (e.g., repairs, maintenance, software updates and enhancements) that need to be carried out on systems of Silver Star Motors EAD Silver Star Motors EAD or on those of service providers, which are necessary in order to ensure that B2B Connect is properly provided or improved.

### § 9 Liability, Indemnification

Silver Star Motors EAD and Partner are liable for themselves and their vicarious agents in case of intent and gross negligence, as well as for slight negligence in case of death or bodily injury.

Furthermore, Silver Star Motors EAD and Partner are liable for slight negligence as follows: Liability consists only in the event of a breach of essential contractual obligations; "essential contractual obligations" are such, where the fulfilment of this obligation is of essential importance for the proper execution of the agreement (cardinal obligations). This liability is limited to the typical direct damage foreseeable at the time the contract is concluded. Insofar as the damage is covered by an insurance policy concluded by the Partner or Silver Star Motors EAD for the damage in question (excluding total insurance), Silver Star Motors EAD or the Partner are only liable for any associated disadvantages of the Partner or Silver Star Motors EAD, e.g. higher insurance premiums or interest rate disadvantages, until the insurance is settled.

Partner is obliged to indemnify Silver Star Motors EAD from all damages, losses, liabilities, claims (including third party claims) and costs (including the appropriate legal fees and costs) arising from a culpable breach of these terms and the transactions contemplated herein (including but not limited to Partner's use of the Seller Center).

### § 10 Duration and termination of the Terms of Use

These Terms of Use replace the previous Terms of Use with relation to the same subject with effect from [..], 2023 and commence on the acceptance of them.

Both Parties can terminate these Terms of Use in writing (textual form suffices with regard to all terminations under this § 10) with a notice period of three months to the end of a month. In any case, these Terms of Use end with the termination of the Authorized Service Agreement between the Parties.

After the termination of the Terms of Use, the provisions on data protection and confidentiality referred to in § 4, 5 and 6 will continue to exist.

In the event of serious breaches of these Terms of Use, such as transferring data that constitutes a breach of the obligation of confidentiality pursuant to § 5, each Party can terminate these Terms of Use without notice. In the event of termination due to a serious breach of contract by a Party, the other Party reserves the right to assert further damage.

Termination in case of discontinuation of the main license: Silver

## Mercedes-Benz-internal use only-draft Review by local legal counsel required

Star Motors EAD rights to provide WebParts Dealer Client and B2B Connect Seller Center to Partner derive from an agreement between MBAG and Silver Star Motors EAD. Silver Star Motors EAD may terminate these Terms of Use upon prior written notice to Partner if its own rights to provide WebParts Dealer Client and B2B Connect Seller Center are terminated / not continued by MBAG.

### **§ 11 Tax**

In case **Silver Star Motors EAD** is liable to pay taxes and customs duties duly allocable to the sale of products posted on provide WebParts Dealer Client and B2B Connect Seller Center by the Partner or to services posted on B2B Connect by the Partner and provided to Customer such as for example digital services taxes, Partner will cover all expenses of **Silver Star Motors EAD** arising from such

taxes and customs duties. The same applies to value added tax owed and not paid by the Partner, for which Silver Star Motors EAD was held liable.

### **§12 Place of Jurisdiction**

These Terms of Use are governed by the law of [seat of Silver Star Motors EAD]. The exclusive place of jurisdiction for disputes arising from these Terms is Sofia,Bulgaria.

### **Appendices to these Terms of Use**

#### **Appendix 1 – Data Protection Agreement**

Appendix 1:

Data Protection Agreement

B2B Connect Platform and related Services

between

[MPC/GD]

Silver Star Motors EAD

("MB X")

and

Authorized Service Partner

("ASP")

(each a "Party", and together the "Parties").

BACKGROUND

- (A) *Whereas*, MB X is a company of the Mercedes-Benz company group and supports the business of the Mercedes-Benz AG in relation to its Dealers ("Dealers" including ISP Customers ("ISP") and Authorized Service Partners) in Germany, Europe (EU) and the rest of the world ("RoW") by offering certain aftersales and marketing related services ("Services", as defined below).
- (B) *Whereas*, offering and providing the Services involves the transfer and processing of Personal Data to and by MB X to provide the Services to ASPs.
- (C) *Whereas*, European and local data protection laws provide for certain requirements with regards to, amongst other things, transferring and processing Personal Data within company groups or distribution or aftersales networks.
- (D) *Whereas*, this Agreement is intended to provide adequate safeguards and protection in the course of national, cross-border, EU-wide as well as world-wide transfer and processing of Personal Data under Applicable Data Protection Laws as defined below.
- (E) *Therefore*, the Parties conclude the following Agreement (hereinafter referred to as "Agreement").

1. DEFINITIONS

1.1 In this agreement, the following terms shall have the following meanings:

- (a) "Personal Data", "Controller", "Processor", "process/processing" "data subject", "technical and organisational measures" and "supervisory authority/authority" shall be interpreted in accordance with the GDPR or the equivalent terminology under Applicable Data Protection Laws. Sub-processor shall have the same meaning as "another processor" in the GDPR or the equivalent terminology under Applicable Data Protection Laws.
- (b) "Agreement" shall mean this Data Protection Agreement.

- (c) “Applicable Data Protection Laws” shall mean the GDPR, any national data protection laws applicable in a European Union member State, or any other national data protection law as applicable to each of the Parties – jointly or separately – when processing data under this Agreement. The fact that a Party has executed this Agreement accordingly shall not have the effect that any data protection law applicable to one Party shall automatically apply to the other Party/Parties and vice-versa. Safe for the terms of this Agreement, the applicability of Applicable Data Protection Laws for any of the Parties shall be determined by the respective laws. Thus, and subject to further provisions and obligations of the Parties as set forth in this Agreement, each Party shall comply with the Applicable Data Protection Laws if and to the extent applicable to it only. For reasons of clarification and by way of example, where reference is made to the statutory rights of data subjects under Art. 12-22 GDPR or the statutory requirements for data processing on behalf under Art. 28 GDPR such rights or requirements shall only apply to controllers falling within the scope of the GDPR.
- (d) “Adequate Country” shall mean any country outside of the EEA that is recognized by the European Commission as providing an adequate level of privacy protection by reason of its domestic law or of the international commitments it has entered into.
- (e) “Data Processing on behalf of a Controller” means the processing of Personal Data that is to be carried out on behalf of a Controller and shall be interpreted in accordance with Article 28 of the GDPR.
- (f) “MBAG” means Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Germany.
- (g) “MB X” means [Silver Star Motors EAD , 52 Chelopeshko shose str., 1839 Sofia, Bulgaria].
- (h) “Clauses” shall mean, collectively, the Clauses on Data Processing on behalf of a Controller and the Controller-to-Controller Clauses.
- (i) “Clauses on Data Processing on behalf of a Controller” shall mean the provisions as set forth in Part B.
- (j) “Joint-Controller Clauses” shall mean the provisions as set forth in Part A. Joint-Controller Clauses shall govern the transfer and use of Personal Data between MB X and ASP whereby the Parties are each acting as Joint Controllers where provided for each of them under Applicable Data Protection Laws.
- (k) “GDPR” shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- (l) “Joint Controllership” means the processing of Personal Data where the purpose of such processing is jointly determined between two or more Controllers and shall be interpreted in accordance with Article 26 of the GDPR.
- (m) “Member State” shall mean a country which is a member state of the EU.
- (n) “Services” shall mean the aftersales related services as further described in the related separate contracts and Parts to this Agreement.

1.2 In this Agreement:

- (a) references to a statutory provision include any subordinate legislation made from time to time under that provision;
- (b) references to this Agreement include the Annexes and Appendices;
- (c) headings shall be ignored in construing this Agreement; and
- (d) if there is any conflict or inconsistency within this Agreement then the conflict or inconsistency shall be resolved by the Clauses taking precedence.

## 2. SCOPE

2.1 The Clauses shall apply as between the Parties in their role as Controller (or joint controller where such a concept exists under Applicable Data Protection Law for the respective Party) or Processor in relation to the relevant Personal Data processed as further defined in the Annexes to Parts A and B.

2.2 In the execution of this Agreement each Party adheres to respectful treatment of the local data protection law's specifics being binding for the other Party.

Given this, each Party shall define whether it can be deemed a Controller or Joint Controller according to Applicable Data Protection Law, more precisely the law being applicable to such Party in this particular context. In case that such law does not provide for the concept of a Joint Controller the concerned Party shall be deemed a Controller hereunder, while the other Party may be deemed a Joint Controller, if applicable. As a consequence, where one of the Parties would be deemed a Joint Controller in the meaning of Applicable Data Protection Law while the other Party would not, the provisions of this Agreement shall be meant to satisfy the respective obligations under Applicable Data Protection Law as applicable to each of the Parties alike. The aforesaid does, however, not limit or otherwise affect the applicability of this Agreement and the obligations resulting from it for each of the Parties.

2.3 Each Party, in its capacity as a Controller or Processor, will oblige sub-processors (if any) to provide at least a similar level of protection and further ensures that the sub-processor will meet MB X's security and privacy guidelines and requirements before entering into an appropriate agreement with a sub-processor.

## 3. MODIFICATIONS AND VARIATIONS

The Parties may update or supplement this Agreement, in accordance with the mechanism agreed upon in the underlying agreement (Terms of Use\_ASP\_B2B Connect).

## 4. TERM AND TERMINATION

4.1 This Agreement shall take effect as of the execution by both Parties by accepting these terms electronically (as part of respective terms and conditions). Each Party to this Agreement shall be bound by the terms and conditions contained in the Agreement from the date such Party has duly executed the Agreement.

4.2 This Agreement will be in effect as long as the contractual relationship (of which this Agreement is part of) between the Parties is terminated or the Services cease to be provided, depending on which event lies further in the future, it being understood that the obligations of the Parties under this Agreement will continue as long as Personal Data of one Party is processed by the other Party.

## 5. NOTICES

Any notice given under this Agreement ("**Notice**") shall be in textual form.

## 6. ASSIGNMENT

ASP may not assign or transfer any of the rights or obligations under this Agreement without the prior written consent of MB X.

## 7. Liability

The Parties shall be liable to each other for any third party claim or other losses or damages for which they are responsible (in particular for damages that have occurred within their respective sphere of influence) and which are arising from the breach of their obligations hereunder and/or other violations of Applicable Data Protection Laws, unless the other party has not been made aware of any such obligations. If one of the Parties is obligated according to Applicable Data Protection Laws to provide full compensation for the damage suffered to a data subject and has done so, such Party shall be entitled to recover from the other Party the part of the compensation corresponding to the other Party's share of responsibility for the damage.

## 8. SEVERABILITY

- 8.1 If any provision in this Agreement shall be held to be illegal, invalid or unenforceable in whole or in part, the legality, validity and enforceability of the remainder of this Agreement shall not be affected.
- 8.2 The Parties agree to supplement the invalid provision whose effect comes as close as possible to the economic objective pursued by the Parties with the invalid provision. The above provisions shall apply mutatis mutandis in the event that the Agreement is incomplete.

## 9. GOVERNING LAW AND PLACE OF JURISDICTION

The place of performance is Sofia [place of business of MB X], and jurisdiction and venue shall lie with the competent courts of Bulgaria [country/jurisdiction of MB X]. The laws of Bulgaria shall apply, to the exclusion of any conflict of law rules. The Parties agree to exclude the application of the uniform United Nations (UN) law of sales that is based on the UN Convention on Contracts for the International Sale of Goods of 11 April 1980.

## 10. RELATION TO SEPARATE AGREEMENTS

- 10.1 This Agreement replaces all data protection regulations previously existing between the Parties in relation to the data processing activities explicitly regulated herein.
- 10.2 Any matter not expressly addressed herein including the liability of the Parties when providing or using respective Services or transmitting respective data for the indicated purposes shall be governed by the terms of any further existing agreements (deriving from the contractual relationship as set out in Section 4.2) between the Parties.
- 10.3 In case of discrepancies between the terms of this Agreement and such other agreements as referred to in Section 10.2, the terms of this Agreement shall prevail.



## PART A

### JOINT-CONTROLLER CLAUSES

#### Preamble

In the context of their business cooperation in the area of B2B Connect, the Parties wish to share personal data for certain business purposes and process it as data controllers within the meaning of data protection law (hereinafter referred to as "Cooperation").

In these Clauses (hereinafter referred to as the "Agreement"), the Parties set out the rights and obligations of the Parties with regard to the processing of personal data carried out in the context of the Cooperation and the respective responsibilities with regard to compliance with the relevant data protection obligations.

Against this background, the Parties enter into the following Agreement:

#### 1. Objective of the Agreement

This Agreement governs the rights and obligations of the Parties (hereinafter also "Controllers") when processing personal data as Joint Controllers.

#### 2. Scope of Processing under Joint Control

2.1 Throughout the Cooperation, the Parties process personal data as Joint Controllers within the meaning of Art. 26 GDPR. The provisions of this Agreement shall apply to all processing activities carried out under a joint controllership in which employees of the controllers or processors commissioned by them process personal data on behalf of the controllers. The scope of the processing as Joint Controllers including the respective roles, responsibilities and competences as well as further details of the processing are set out in Annex 1.

2.2 The information in Annex 1 is substantiated by the process and activity descriptions in the contracts concluded in parallel by the Parties (e.g. service contracts), including the information texts provided in parallel, to which reference is made.

#### 3. Duties of the Controllers

3.1 The Controllers shall carry out the processing of personal data in accordance with the relevant provisions of the Applicable Data Protection Laws and shall be jointly responsible for compliance with the GDPR provisions relevant for Joint Controllers with regard to the processing activities covered by this Agreement and as set out in this Agreement. In particular, they shall ensure that only personal data necessary for the processing operations and purposes described in Annex 1 is collected. In addition, the Controllers shall observe the principle of data minimization (cf. Art. 5 (1) (c) GDPR).

3.2 Each Controller is internally responsible for the lawfulness of the collection and processing of personal data within the scope of the tasks and responsibilities assigned to it below and in Annex 1.

3.3 Controllers shall ensure that all persons involved in the processing of personal data in the context of the Cooperation are or will be bound by confidentiality and data secrecy obligations prior to accessing such data, with effect during their activity as well as after the termination of their activities. They shall ensure that the relevant persons are instructed in the data protection provisions relevant to them.

3.4 Controllers shall store personal data in a structured, commonly used and machine-readable format. Personal data must be accurate and, where necessary, kept up to date. The Controllers shall take all measures to implement this.

- 3.5 Controllers shall inform each other immediately and fully if they discover errors or irregularities with regard to data protection provisions during the review of processing activities.
- 3.6 Documentations which serve as proof of the proper processing (cf. Art. 5 (2) GDPR) shall be kept by each Party in line with its legal powers and obligations beyond the end of the Agreement.

#### **4. Technical and Organizational Measures**

- 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, Controllers shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, as appropriate, the following:
- the ability to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on an ongoing basis;
  - the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident;
  - a procedure for periodically reviewing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing; and
  - a procedure for proper compliance with the data protection principles through technology and through data protection-friendly default settings pursuant (cf. Art. 25 GDPR).

The Controllers may specify further requirements separately.

- 4.2 The Controllers shall take all necessary technical and organizational measures to ensure that the rights of the data subjects, in particular pursuant to Art. 12 – 22 GDPR, may be exercised at all times in accordance with the legal requirements. If necessary, the Controllers shall agree on the concrete design of the measures and jointly decide on their implementation.
- 4.3 The implementation, default settings and operation of the systems shall be carried out in compliance with the requirements of the Applicable Data Protection Laws, in particular in compliance with the principles of privacy by design and privacy by default, as well as using appropriate technical and organizational measures in accordance with the state of the art.

#### **5. Responsibility for Compliance with Data Protection Laws and Data Subjects' Rights**

- 5.1 Data subjects may assert data subject rights to which they are entitled under Art. 12 – 22 GDPR vis-à-vis any of the Controllers, who in principle remain responsible for the fulfilment of the respective rights in the external relationship.
- 5.2 Unless otherwise provided for in Annex 1 or in another context, the Controller who originally collected the personal data concerned from the data subject before transferring it to the other Controller for further processing, or who had or has a direct contractual relationship with the data subject, shall remain the central point of contact for the data subjects and shall support the Controller subject to the GDPR with their responsibilities regarding the fulfilment of the data subjects' rights pursuant to Art. 12 – 22 GDPR in the internal relationship. Such support shall be provided in a way that enables the other Controller to fully fulfill those rights.
- 5.3 The Controllers will support each other to an appropriate extent in the fulfilment of the data subject rights, inform each other about corresponding requests and provide each other with all information necessary in due time. If personal data is to be deleted the Parties shall inform each other in due time in advance. The other Party may object to the deletion for a legitimate reason, for example if it has a legal obligation to retain the data.
- 5.4 Data subjects shall be provided with information about the processing in accordance with Art. 13 and

14 GDPR. The Controllers shall support each other in fulfilling the information obligations and provide each other with the necessary information on the relevant data processing activities.

- 5.5 Unless otherwise provided for in Annex 1 or in another context, the Controller who originally collected the personal data concerned from the data subject before transferring it to the other Controller for further processing, or who has had or has a direct contractual relationship with the data subject, shall remain responsible for providing the data subjects with information on the main content of these regulations. To this end, the Controller may provide data subjects with the provisions of this Section 6 upon request.
- 5.6 Each of the Controllers is responsible for the reporting and notification obligations resulting from potential data breaches vis-à-vis the supervisory authority and the data subjects affected by a personal data breach for their respective area of responsibility (cf. Art. 33, 34 GDPR). In the event of a reportable incident with regard to the processing activities covered by this Agreement, the Controllers shall inform each other without delay and before reporting the incident to a supervisory authority or informing data subjects. The Controllers shall support each other to the best of their ability in clarifying the facts and taking appropriate measures to protect the data subjects. The decision as to the necessity, content and scope of the measures to be taken shall be taken by the respective Controller who is obliged to notify.
- 5.7 The Parties shall assist each other, as necessary and upon request, in the preparation of a data protection impact assessment (cf. Art. 35 GDPR) or the consultation of the authority (cf. Art. 36 GDPR). The Parties shall provide each other with the information necessary for this from their respective spheres of activity in due time.
- 5.8 Each Controller shall maintain a record of processing activities in its own responsibility. Controllers shall provide each other with the information necessary to maintain an appropriate record of processing activities.
- 5.9 Documents serving as evidence of proper data processing (see section 5.6) shall be retained by each Party beyond the end of the contractual relationship. Controllers shall ensure that they comply with all existing legal obligations to retain the personal data concerned.
- 5.10 Unless otherwise agreed, each Controller shall bear its own costs, if any, incurred in the performance of its obligations under this Agreement, without being entitled to claim any remuneration from the other Controller for the performance of such obligations.

## **6. Processor**

- 6.1 Each Controller is entitled to use processors.
- 6.2 If the Controller engages a processor for the processing activities being subject to this Agreement, this shall only be done to the extent that the requirements under the Applicable Data Protection Laws are met.
- 6.3 Controllers shall make available to each other, upon request a list of processors involved in data processing activities pursuant to this Agreement. The Controllers shall inform the other Controllers of any intended changes regarding the addition or replacement of other processors upon request.
- 6.4 This does not apply in cases where the Controllers commission third parties for ancillary services. These include, but are not limited to, postal, telecommunications, shipping and receiving services and facility management services. Controllers remain obligated to implement appropriate contractual arrangements and obligations with the respective service providers in accordance with applicable legal requirements and to provide for appropriate control measures in relation to the security of personal data.

## **7. Processing within and outside the European Economic Area**

- 7.1 In principle, processing takes place in a member state of the European Union, in a country of the European Economic Area (EEA) or in a country with an adequate level of protection. Processing activities in other countries outside the EEA are permitted, provided that the applicable provisions on the international transfer of personal data are complied with.
- 7.3 If and insofar as there are no guarantees for the transfer of personal data to third countries within the meaning of Art. 44 et seq. GDPR, such as Binding Corporate Rules pursuant to Art. 47 GDPR, the provisions of the EU Standard Contractual Clauses in Annex 2 apply.

## **8. Liability**

- 8.1 The Controllers shall be liable to data subjects pursuant to statutory provisions.
- 8.2 The Controllers shall be liable in the internal relationship insofar as each of them bear a share of the responsibility for the cause giving rise to liability. This shall also apply with regard to a fine imposed on a Controller for a breach of data protection provisions, provided that the Controller subject to the fine must first have exhausted all legal remedies against the official decision. If a Controller then remains subject to a fine that does not correspond to its internal share of responsibility for the breach, the respective other Controller is obligated to indemnify the Controller concerned from the fine to the extent that it bears responsibility for the breach sanctioned by the fine.
- 8.3 Any limitations of liability agreed in supplementary contracts for the relevant services shall apply accordingly.

## **9. Power of Attorney**

- 9.1 MB X has been authorized by MBAG to execute these Joint-Controller Clauses (including its Annexes) also in the name and on behalf of MBAG and, thus, to render MBAG a party to these Joint Controller Clauses as another Controller with the role as specified in Annex 1. If MBAG is not indicated as Controller in Annex 1 (or Annex 2) below, MBAG shall not become a Party to this Agreement in this respect. ASP herewith confirms and consents to MBAG becoming a Party here-under being awarded any and all rights and obligations as a Controller under this Part A including its Annexes (excluding other parts of the Agreement unless otherwise stipulated herein) and, thus, becoming a Controller hereunder.
- 9.2 MB X shall be entitled to inform MBAG on the ASPs to which respective contractual relationships have been established, including company name, address and content of the respective agreement, and provide sufficient proof thereof upon MBAG's request e.g. by providing copies of the executed agreement and this Part A in particular.
-

**Annex 1: Roles, Tasks and Scope of the Collaboration***1. Business Analytics related processing activities*

Procedure	Purpose / Scope	Roles and Tasks	Data Categories and Data Subjects
Ticket Support for ISPs in the Seller Center	Providing ASPs the option to supporting ISPs with tickets in the Seller Center and account opening requests.	<p>MB X: Controller</p> <p>Provides option for ASP to support ISPs with tickets in the Seller Center and makes ticket and request information available to ASP upon notice to ISP; is responsible for technical processing of ticket information</p> <p>ASP: Controller</p> <p>Supports ticket / request for ISP in collaboration with ISP; is responsible for properly handling information provided and correct processing</p>	<p>ISP data: ISP company name, user name, user ID, address, email, telephone, ticket or request details (date, subject)</p> <p>ASP data: company name, user name, user ID, address, email, telephone</p>
Business Analytics	<p>Sales data acquired through the operation of the B2B Connect Platform shall be used to analyse business operations and to provide aggregated reports to MBAG, MB X and ASP.</p> <p>Reports are usually created by automated calculations (application based).</p> <p>In exceptional cases the data is merged with data from other sources (e.g. another database from another MBAG department) to run further analysis.</p> <p>MBAG and its employees operate strictly according to the need-to-know principle.</p>	<p>MBAG: Controller</p> <p>Operates business logic and hosts data base with business data, creates aggregated evaluations/reports based on the provided data for itself, MB X and ASP.</p> <p>MB X: Controller</p> <p>Allows transmission of B2B platform transaction related data to be used for the above processes; receives aggregated reports</p> <p>ASP: Controller</p> <p>Allows transmission of B2B platform transaction related data to be used for the above processes; receives aggregated reports</p>	<p>ISP data: ISP company name, user name, user ID, address, email, telephone, order details (date of order, parts/services ordered, order quantity, sales, orders not placed (lost sales), frequency of use of B2B Connect Platform/aftersales related Services, delivery times)</p> <p>ASP data: company name, user name, user ID, address, email, telephone</p>

*2. Recipients*

Restricted individuals with dedicated roles to whom Personal Data will only be disclosed on a need-to-know-basis as required in order to carrying out their respective managerial responsibilities (e.g. contractors, including those for HR, IT and finance (where appropriate)); group entities, consultants, auditors, accountants; financial organisations; law enforcement agencies, government agencies, regulatory authorities.

**Annex 2: EU Standard Contractual Clauses****STANDARD CONTRACTUAL CLAUSES****SECTION I***Clause 1****Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
- ( ) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A (hereinafter each “data exporter”), and
  - (i) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2****Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3****Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (iii) Clause 8.5(e) and Clause 8.9(b);
  - (iv) (intentionally left blank)
  - (v) Clause 12(a) and (d);
  - (vi) Clause 13;

- (vii) Clause 15.1(c), (d) and (e);
- (viii) Clause 16(e);
- (ix) Clause 18(a) and (b).

- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7*

***Docking clause***

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES***Clause 8****Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (x) where it has obtained the data subject's prior consent;
- (xi) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (xii) (where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2 Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- (xiii) of its identity and contact details;
- (xiv) of the categories of personal data processed;
- (xv) of the right to obtain a copy of these Clauses;
- (xvi) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.



- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

#### **8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

#### **8.5 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

#### **8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include

restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

### **8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (xvii) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (xviii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (xix) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (xx) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (xxi) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (xxii) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

### **8.9 Documentation and compliance**

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

*Clause 9*

*(Intentionally left blank)*

*Clause 10*

### ***Data subject rights***

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to

facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

- (b) In particular, upon request by the data subject the data importer shall, free of charge:
- (xxiii) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - (xxiv) rectify inaccurate or incomplete data concerning the data subject;
  - (xxv) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
- (xxvi) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (xxvii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### *Clause 11*

#### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

***Liability***

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES***Clause 14****Local laws and practices affecting compliance with the Clauses***

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15****Obligations of the data importer in case of access by public authorities***

**15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS***Clause 16****Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17****Governing law***

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

*Clause 18****Choice of forum and jurisdiction***

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

## EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.



**ANNEX I**

**A.LIST OF PARTIES**

**Data exporter(s):**

1. Name: Mercedes-Benz AG

Address: Mercedesstraße 120

Contact person's name, position and contact details: /

Activities relevant to the data transferred under these Clauses: see B. below

Signature and date: see section 5 of this Part A

Role (controller/processor): Controller

**Data importer(s):**

1. Name: ASP (see rubrum of the Agreement)

Address: see rubrum of the Agreement

Contact person's name, position and contact details: /

Activities relevant to the data transferred under these Clauses: see B. below

Signature and date: see sign up process details and documentation

Role (controller/processor): Controller

**B.DESCRPTION OF TRANSFER**

*Categories of data subjects whose personal data is transfer*

See Annex 1 to Part A

*Categories of personal data transferred*

See Annex 1 to Part A

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

Not applicable

*The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).*

Continuous basis

*Nature of the processing*

See Annex 1 to Part A

*Purpose(s) of the data transfer and further processing*

See Annex 1 to Part A

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

<u>Customer data</u> : ISP/ISP employee such as company title, user name, user ID, address, email, telephone, order details (date of order, parts/services ordered, order quantity, sales, orders not placed (lost sales), frequency of use of B2B Connect Platform, delivery times)	Definition of a retention period from the business process	Anonymize after 2 years after placed order, deletion after further 3 years after reports are created (reports created on monthly and quarterly basis)
	Deletion rule with specific starting date	Anonymize after 2 years after placed order, deletion after further 3 years after generating the monthly or quarterly reports

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Not applicable

Internal

Mercedes-Benz-internal use only-draft  
Review by local legal counsel required

### **C.COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Königstraße 10 a, 70173 Stuttgart*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

## EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

For B2B Connect related processing activities (including Business Analytics and Campaign/Marketing Support) the following TOMs shall apply:

1. Access control (physical)	Yes	No	Not applicable
The areas with systems where applications process personal data are divided into different security zones	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specification of authorized persons, including scope of authority regarding physical access to relevant rooms or areas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admittance authorization IDs issued	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations for visitors in place	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations governing keys implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All individuals recorded in and out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical protection of company premises (e.g. fence, external walls, checkpoints)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure entrance (e.g. locking system, ID readers)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Burglar-resistant windows	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Surveillance installation (e.g. alarm system, CCTV)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separation system (e.g. turnstiles, double-door system)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Documentation of physical protection measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Access control (systems)	Yes	No	Not applicable
Documented security concept to enter (log-in) the application	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Use of the Global Authentication Service (GAS)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular synchronization with Corporate Directory	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Use of the Secure Application Gateway (SAGW/WCP)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Access authority specified and checked	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User identified and authorization verified	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User identity management system implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Special authentication process (e.g. chip cards, biometric access control)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Appropriate password protection (binding requirements for secure passwords, encrypted storage)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access attempts monitored, including response to security issues	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolation of internal network (e.g. by using VPN, firewalls)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Immediate deletion of accounts of former employees	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special security software (e.g. anti-malware, intrusion detection)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations for visitors in place	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Mercedes-Benz-internal use only-draft

### Review by local legal counsel required

Remote access rules and regulations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-------------------------------------	-------------------------------------	--------------------------	--------------------------

3. Access control (user rights)	Yes	No	Not applicable
Authorization and roles concept implemented for applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User accounts required for data access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular review of authorizations	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Access restrictions imposed (based on principles of need-to-know and least privilege)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Additional passwords (based on the 4-eyes-principle) for particularly important functions (e.g. system admin)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Securing of multi-client capability of the system	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separated and multi-client capable databases	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separation of development, test, integration and productive environment	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separation of productive and archiving environment	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Read-access logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Write-access logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unauthorized access attempts logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Implementation of retention periods for data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Disclosure control	Yes	No	Not applicable
Data transfer encrypted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data retention encrypted	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mobile terminals encrypted (e.g. hard disk encryption)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data forwarding or transfer logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forms of data forwarding fully documented (e.g. printout, data media, automated transfer)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interfaces documented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restriction of rights for data transfer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Plausibility, completeness, and accuracy checks regarding data carried out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USB interface deactivation	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile device handling regulations implemented	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data carrier disposal regulations implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Protection against data manipulation (Malware protection)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Input control	Yes	No	Not applicable
System logging/recording ensured	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular evaluation of logfiles/protocols	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Segregation of Duties (SoD) ensured (SoD matrix defined and procedures implemented)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Authorization to enter, alter or delete data documented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Entry/Alteration of data completely logged/recorded	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Entry/Alteration of data partly logged/recorded	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alteration/Deletion of data prohibited	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Electronic signature to ensure authenticity of data alteration	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Mercedes-Benz-internal use only-draft

### Review by local legal counsel required

6. Job control	Yes	No	Not applicable
Mercedes-Benz's standard agreement on data processing on behalf has been agreed on	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data processor's standard agreement on data processing on behalf has been agreed on	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standard Contractual Clauses of the EU Commission has been agreed on for data processing on behalf by processors in third countries	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Responsibilities of data controller and data processor are strictly regulated / separated	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules specified to adjust / change instructions given to the data processor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
On-site controls have been conducted and documented by the data controller	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted self-assessments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted approved certifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted list of subcontractors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Checks on subcontractors by processor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

7. Availability control	Yes	No	Not applicable
System condition regularly checked (monitoring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup and recovery plan in place (regular data backups)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data archiving strategy implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Documented contingency plans (business continuity, disaster recovery)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contingency plans regularly tested	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Presence of redundant IT systems assessed (servers, storage, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fully operational physical protection systems in place (fire protection, energy, A/C)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. Procedures for the regular Review, Assessment and Evaluation of the Effectiveness of the Technical and Organisational Measures taken	Yes	No	Not applicable
Regular checks of the system status (monitoring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Revision of the implementation of the described measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Description of applicable data protection requirements in binding guidelines and instructions for action	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Involvement of the data protection officer in relevant new data processing procedures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Mercedes-Benz-internal use only-draft

### Review by local legal counsel required

For Webparts related processing activities (including Business Analytics and Campaign/Marketing Support) the following TOMs shall apply:

1. Access control (physical)	Yes	No	Not applicable
The areas with systems where applications process personal data are divided into different security zones	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specification of authorized persons, including scope of authority regarding physical access to relevant rooms or areas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admittance authorization IDs issued	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations for visitors in place	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations governing keys implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All individuals recorded in and out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical protection of company premises (e.g. fence, external walls, checkpoints)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure entrance (e.g. locking system, ID readers)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Burglar-resistant windows	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Surveillance installation (e.g. alarm system, CCTV)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separation system (e.g. turnstiles, double-door system)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Documentation of physical protection measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Access control (systems)	Yes	No	Not applicable
Documented security concept to enter (log-in) the application	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Use of the Global Authentication Service (GAS)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular synchronization with Corporate Directory	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Use of the Secure Application Gateway (SAGW/WCP)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access authority specified and checked	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User identified and authorization verified	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User identity management system implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Special authentication process (e.g. chip cards, biometric access control)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Appropriate password protection (binding requirements for secure passwords, encrypted storage)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access attempts monitored, including response to security issues	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolation of internal network (e.g. by using VPN, firewalls)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Immediate deletion of accounts of former employees	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Special security software (e.g. anti-malware, intrusion detection)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rules and regulations for visitors in place	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remote access rules and regulations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Access control (user rights)	Yes	No	Not applicable
Authorization and roles concept implemented for applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User accounts required for data access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular review of authorizations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access restrictions imposed (based on principles of need-to-know and least privilege)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Mercedes-Benz-internal use only-draft

### Review by local legal counsel required

Additional passwords (based on the 4-eyes-principle) for particularly important functions (e.g. system admin)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Securing of multi-client capability of the system	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separated and multi-client capable databases	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Separation of development, test, integration and productive environment	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separation of productive and archiving environment	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Read-access logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Write-access logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unauthorized access attempts logged	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Implementation of retention periods for data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. Disclosure control	Yes	No	Not applicable
Data transfer encrypted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data retention encrypted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mobile terminals encrypted (e.g. hard disk encryption)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data forwarding or transfer logged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forms of data forwarding fully documented (e.g. printout, data media, automated transfer)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interfaces documented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restriction of rights for data transfer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Plausibility, completeness, and accuracy checks regarding data carried out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USB interface deactivation	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile device handling regulations implemented	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data carrier disposal regulations implemented	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Protection against data manipulation (Malware protection)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5. Input control	Yes	No	Not applicable
System logging/recording ensured	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regular evaluation of logfiles/protocols	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Segregation of Duties (SoD) ensured (SoD matrix defined and procedures implemented)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Authorization to enter, alter or delete data documented	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Entry/Alteration of data completely logged/recorded	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Entry/Alteration of data partly logged/recorded	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alteration/Deletion of data prohibited	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Electronic signature to ensure authenticity of data alteration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Job control	Yes	No	Not applicable
Mercedes-Benz's standard agreement on data processing on behalf has been agreed on	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor's standard agreement on data processing on behalf has been agreed on	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Standard Contractual Clauses of the EU Commission has been agreed on for data processing on behalf by processors in third countries	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Responsibilities of data controller and data processor are strictly regulated / separated	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Mercedes-Benz-internal use only-draft

### Review by local legal counsel required

Rules specified to adjust / change instructions given to the data processor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
On-site controls have been conducted and documented by the data controller	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted self-assessments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted approved certifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data processor submitted list of subcontractors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Checks on subcontractors by processor	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

7. Availability control	Yes	No	Not applicable
System condition regularly checked (monitoring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup and recovery plan in place (regular data backups)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data archiving strategy implemented	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Documented contingency plans (business continuity, disaster recovery)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contingency plans regularly tested	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Presence of redundant IT systems assessed (servers, storage, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fully operational physical protection systems in place (fire protection, energy, A/C)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. Procedures for the regular Review, Assessment and Evaluation of the Effectiveness of the Technical and Organisational Measures taken	Yes	No	Not applicable
Regular checks of the system status (monitoring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Revision of the implementation of the described measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Description of applicable data protection requirements in binding guidelines and instructions for action	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Involvement of the data protection officer in relevant new data processing procedures	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

---

**Mercedes-Benz-internal use only-draft**  
**Review by local legal counsel required**

**PART B**

**Clauses on Data Processing on behalf of a Controller**

**Preamble**

These Clauses on Data Processing on behalf of a Controller (“**Clauses Part B**”) specify the Parties’ obligations with regard to data protection which result from the Data Processing on behalf of a Controller as described below. These Clauses in Part B apply to any activity that relates to these processing operations and in the course of which employees of the Processor or third parties commissioned by the Processor might get in contact with Personal Data of the Controller. These Clauses shall, however, be limited in its application to circumstances, where one of the Parties is acting as a Processor in the meaning of Art. 28 GDPR vis-à-vis the other Party. Outside of this scope these Clauses shall not apply.

**1. Roles and Responsibilities**

The Controller relies on the processing of Personal Data to perform its after-sales business. For this purpose, Processor provides services to Controller as described in [Annex 1](#).

**2. Subject matter and responsibility**

Processor processes Personal Data on behalf of Controller. Subject matter of the commissioning are activities as specified below or within any additional service agreement or order form. Within the scope of these Clauses Part B, Controller shall be solely responsible for compliance with Applicable Data Protection Law, in particular the lawfulness of the transfer of data to Processor, the processing of the data through Processor and any subsequent processing of data in the course of the Services.

**3. Specification of the commissioning**

- 3.1 Purpose, type and extent of the commissioned collection, processing and/or use of Personal Data are further described in [Annex 1](#).
- 3.2 The type and categories of the collected and/or used Personal Data as well as the category of data subjects who are subject to the handling of Personal Data hereunder are further described in [Annex 1](#).

**4. Controller’s right to issue instructions**

- 4.1 Within the scope of the commissioning, Controller reserves a right to issue instructions concerning the type, extent and procedure of data processing which it may specify by issuing individual instructions. These are conclusively determined and are to be exercised through the settings and functions as provided by the provided applications and systems. Instructions leading to changes of the agreed subject matter of processing and the procedures have to be agreed upon and shall then be documented.
- 4.2 Processor will inform Controller of any instruction that it deems to be in violation of data protection requirements. Processor may then postpone the execution of the relevant instruction until it is confirmed or changed by Controller in writing (incl. via e-mail).
- 4.3 Except for any deviating agreement between the Parties in writing, Controller’s management or other authorized representative only are authorized to issue instructions on the side of Controller which shall be in writing (incl. via e-mail).
- 4.4 Authorized to receive instructions on the side of Processor is the “Data Protection Coordinator for Silver Star EAD” which can be contacted via [dpo@silverstarmotors.eu](mailto:dpo@silverstarmotors.eu).

**5. Obligations of Processor**

- 5.1 Processor shall collect or process data only as commissioned by Controller and in compliance with the instructions of Controller, unless the Processor is required to do so by European Union or Member State law, or any other Applicable Data

## **Mercedes-Benz-internal use only-draft**

### **Review by local legal counsel required**

Protection Laws to which the Processor is subject to; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Processor will rectify, delete or block the data processed on behalf of Controller only as instructed by Controller. If a data subject contacts Processor with a request for correction or deletion of its data, Processor shall forward the request to Controller.

- 5.2 Unless prohibited by applicable law or a legally-binding request of law enforcement, Processor shall promptly notify Controller of any request by a data protection supervisory authority, law enforcement authority or other public authority for access to or seizure of Personal Data. In addition, to the extent permitted by law, Processor shall use all reasonably available measures to defend against such action or allow Controller to do so in lieu of and on behalf of Processor, and if it so chooses, seek a protective order or allow Controller to do so on Processor's behalf. In any case, Processor shall reasonably cooperate with Controller in such defence.
- 5.3 Before granting access to Personal Data, Processor will oblige persons employed in processing Personal Data on data secrecy and confidentiality and familiarize them with the provisions as set forth in these Clauses Part B and data protection obligations applicable to them. To the extent that Processor is processing PersonalData subject to professional secrecy or other special confidentiality obligations (e.g. data subject to the secrecy of telecommunications) such obligation shall also include these specific circumstances and related obligations.
- 5.4 Insofar as required by Applicable Data Protection Law, Processor will appoint a data protection officer and will forward its contact details to Controller and shall without undue delay report to Controller any changes and updates during the term of this Agreement.
- 5.5 Processor will without undue delay notify Controller of violations of instructions or of provisions for the protection of Controller's Personal Data by Processor or a person employed by Processor.

Processor acknowledges that Controller may be obliged to document breaches of the protection of Personal Data and, if necessary, inform a supervisory authority, respectively the data subject, within 72 hours on such breach. If and insofar as it has come to such breaches, Processor will assist the Controller with compliance of its reporting obligations in a proper manner to allow for the Controller to timely perform its obligations hereunder. Processor will inform the breach to the Controller and give at least the following information if and to the extent available to Processor: (a) description of the kind of the breach, the category and the approximate amount of data subjects and datasets involved, (b) name and contact of a contact person for further information, (c) description on the probable consequences of the breach, (d) description of the taken measures in order to remedy or reduce the breach.

Furthermore, Processor shall without undue delay inform Controller of serious disruptions of the normal course of operations, any suspicions of data protection violations or other irregularities in processing the data of Controller.

- 5.6 Processor will inform Controller of any monitoring activity of and measures taken by the supervisory authority with regard to the processing of Personal Data of the Controller.
- 5.7 Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible and reasonable, for the fulfilment of the Controller's obligation towards data subjects, e.g. the information to and access of the data subjects, rectification and erasure of data, restriction of processing or the right to data portability and right to object, if applicable.
- 5.8 Processor assists with the preparation of a data protection impact assessment and, where appropriate, assists with the prior consultation of the supervisory authority. On Controller's request, Processor shall disclose the required information and documents to Controller.
- 5.9 The Parties shall come to an agreement regarding any additional costs that are incurred in accordance with 5.7 and 5.8 above. There shall be no obligation to bear the costs for such services to be rendered by MB X which MB X is or would be obliged to perform regardless of the existence of this commissioning under statutory law.
- 5.10 Processor shall monitor the compliance with obligations specified above during the execution of the commissioned data processing.
- 5.11 Processor shall maintain a record of processing activities carried out on behalf of the Controller.

## **6. Security of Processing**

## **Mercedes-Benz-internal use only-draft**

### **Review by local legal counsel required**

- 6.1 Processor takes all appropriate technical and organisational measures in order to ensure a level of security appropriate to the risk and assist the Controller in ensuring compliance with Applicable Data Protection Laws.

Thus, within its scope of responsibility, Processor will set up its internal organization in accordance with all applicable data protection and data security requirements. Processor shall take, maintain and control technical and organizational measures to ensure reasonable protection of Controller's data against misuse and loss in accordance with the requirements according to applicable laws.

- 6.2 In this connection, Processor shall provide for a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This includes appropriate measures on e.g. entrance control, user control, access control, transmission control, input control, job control, availability control as well as separation by purpose and, inter alia as appropriate, the pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 6.3 Further specifications on the technical and organizational measures result from [Annex 2](#).
- 6.4 Technical and organizational measures are subject to technical progress and development. The Processor may implement adequate alternative measures. These must not, however, fall short of the level of security provided by the specified measures. Any material changes, however, must be documented.

## **7. Rights and obligations of Controller**

- 7.1 Controller and Processor shall each be responsible for compliance with the respective statutory data protection law as it applies to the one or the other with regard to the Personal Data that are to be processed hereunder.
- 7.2 Data subjects will have various rights with respect to the Personal Data held by Controller (and Processor on its behalf). As it will be in any case also the Controller who has a direct relationship with the data subject, Controller shall ensure proper fulfillment of the relevant data subjects rights, in particular to properly inform data subjects on the roles and tasks performed by the parties in accordance with Applicable Data Protection Laws , e.g. by providing access to the actual version of the relevant privacy policy for customers.
- 7.3 Controller shall specify the measures for returning the provided data media and/or deletion of recorded data after the termination of the commissioning. If no specifications are issued, data shall be handed over to Controller or destroyed. Insofar as data are deleted in accordance with particular specifications, Processor shall confirm such deletion to Controller specifying the date on which such deletion has been effected upon request of the Controller.

## **8. Audit**

- 8.1 Controller or his appointed representative have the right to control the compliance of any and all instructions and requirements set forth in this Agreement as well as under Applicable Data Protection Law, including regular inspections. Processor undertakes to permit such controls and to support Controller as well as provide necessary information.
- 8.2 Controller shall primarily pursue his control obligations by demanding respective self-audits by the data protection officer of the Processor's data protection organisation and/or certifications of independent auditors. The Controller reserves the right to carry out additional on-site inspections if necessary according to Applicable Data Protection Law.
- 8.3 Audits by Controller in accordance with section 8.1 and 8.2 above shall take place during regular business hours, shall not disturb standard internal operations and be notified reasonably in advance.
- 8.4 Upon Controller's written request Processor shall provide Controller within a reasonable period of time any information and make the documentation available as necessary for the auditing.

## **9. Sub-Processors**

- 9.1 Processor shall be entitled to use sub-processors for fulfilling its contractual obligations.

**Mercedes-Benz-internal use only-draft**  
**Review by local legal counsel required**

- 9.2 Processor shall ensure by entering into pursuant agreements with sub-processors to impose at least substantially the same obligations on sub-processors which Processor has assumed according to these Clauses in Part B prior to sub-processor being granted access to Controller's Personal Data during performance.
- 9.3 To the extent that Processor involves sub-processors Annex 1 contains further information on the involved sub-processors per procedure. Additionally, involved sub-processors are listed in Annex 3. Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes, whereas Controller has to present reasonable grounds for such an objection. If Controller still does not approve of a new sub-processor, then Controller and Processor may terminate the affected parts of the Services without penalty by providing written notice of termination.
- 9.4 This section 9 shall not apply in cases where Processor subcontracts ancillary services to third parties; such ancillary services shall include, but not be limited to mail, communication, shipping and receiving services and caretaking services.

**10. Territory and international data transfers**

- 10.1 To the extent that international data transfers (if any, including data transfers in relation to sub-processors) will not be covered by the Mercedes-Benz Data Protection Directive EU A 17.4 the Parties (also in relation to sub-processors) shall enter into the respective EU Standard Contractual Clauses where required.
- 10.2 Where applicable, the terms of the EU Standard Contractual Clauses (including its Annexes) shall prevail over any conflicting clauses in the remainder of these Clauses Part B and the entire Agreement. For the avoidance of doubt, provisions in the remainder of these Clauses Part B as well as the entire Agreement that merely go beyond the terms of EU Standard Contractual Clauses without contradicting them shall remain valid.

**11. Liability**

Without prejudice to Section 7 within the main body of this Agreement, Controller shall be liable for damages and shall indemnify Processor against any claims of third parties or other damages and liabilities, including the consequences of supervisory authority orders or fines, resulting from (i) the Controller's breach of its obligations under this Agreement and/or other breaches of applicable data protection laws, and/or (ii) the Processor's breach of applicable data protection laws, insofar as these are based on the proper execution of the provisions of this Agreement or other instructions of the Controller. This shall not apply if the Controller is not responsible for the circumstances giving rise to liability.

Mercedes-Benz-internal use only-draft  
Review by local legal counsel required

**Annex 1: Roles, Tasks and Scope of the Collaboration**

*1. B2B Connect Platform related processing activities*

Procedure	Purpose / Scope	Roles and Tasks	Data Categories and Data Subjects
System Support for B2B Connect Platform Services	Providing user support to employees of ASP (via Ticketing Tool / Call Center)	<p>MB X: Processor (MBAG: Subprocessor)</p> <p>Provides support to ASPs respectively</p> <p>ASP: Controller</p> <p>Use WebParts including user support</p>	ASP data: account data including customer name / company name, customer employee name and customer contact data, customer address, support ticket / incident related information, information on aftersales services system use data including transactional and related ISP data including ISP company title, employee names or purchase order related data (where necessary)

*2. Business Analytics*

Procedure	Purpose / Scope	Roles and Tasks	Data Categories and Data Subjects
Display, reporting and analytics	Displaying ISP transaction data in the B2B Connect Seller Center, providing reports and analytics	<p>MB X: Processor (MBAG: Subprocessor)</p> <p>Displays ISP transaction data in the B2B Connect Seller Center, and provides reports and analytics upon request of ASP</p> <p>ASP: Controller</p> <p>Use WebParts including data display, reporting and analytics</p>	<p>ISP data: ISP company name, user name, user ID, order details (date of order, parts/services ordered, order quantity, sales, orders not placed (lost sales), frequency of use of B2B Connect Platform/ aftersales related Services, delivery times), analytics and reports based on above sales figures</p> <p>ASP data: company name, user name, user ID</p>
Campaign Proposal Services (in case that such a service is requested by MB X and/or ASP; otherwise not applicable)	MBAG and MB X (if applicable) use provided data to run business analytics and creation of related marketing campaigns for MB X and ASPs and support with operating of marketing campaigns. This typically includes for MBAG to provide marketing materials including ISP lists (e.g. with leads) to MB X or ASPs in order to allow for them to contact ISPs via different direct marketing channels (if applicable in the particular market), including transmitting of marketing materials + dealer lists to MB X or ASPs for this purpose.	<p>MBAG: Processor</p> <p>Hosts data base with business analytics data; operates applications and creates marketing campaigns based on the provided data for MB X and ASPs to enable them to contact ISPs via different direct marketing channels. Transmits marketing materials + ISP lists to MB X and/or ASPs for this purpose.</p> <p>MB X: Controller</p> <p>Receive ISP lists + marketing materials for marketing campaigns</p>	<p>ISP data: ISP company name, user name, user ID, address, email, telephone, order details (date of order, parts/services ordered, order quantity, sales, orders not placed (lost sales), frequency of use of B2B Connect Platform/ aftersales related Services, delivery times)</p> <p>ASP data: company name, user name, user ID, address, email, telephone</p>

Mercedes-Benz-internal use only-draft  
Review by local legal counsel required

		<p>(marketing campaigns will be operated by MB X in its sole responsibility, if applicable)</p> <p>May provide similar services to ASPs (in this case acting as a processor to ASPs as well)</p> <p>ASP: Controller</p> <p>Receive ISP lists + marketing materials for marketing campaigns (marketing campaigns will be operated by the ASP in its sole responsibility)</p>	
<p>Direct Marketing Campaign Services (in case that such a service is requested by ASP; otherwise not applicable)</p>	<p>Optionally when ordered by an ASP MB X may support the sending out of marketing material to customers by providing a dedicated web-service for ASPs to upload end-customer contact data and MB X to distribute campaigns in the name and on behalf of the ASP; also, MB X may support ASP with marketing support services by contacting ISP through MB callcenter</p>	<p>MB X: Processor</p> <p>MB X may send out marketing campaigns (emails) in the name and on behalf of ASP (or involve MBAG or another sub-processor for that matter). In this case, MB X will provide an interface via which ASP may transmit end-customer data (names, email-address) to MB X.</p> <p>MB X will then process the data transmitted for sending out of marketing emails (also via third party service providers of MB X).</p> <p>Optionally, MB X may contact ISPs through MB callcenter and follow up on prior business transactions</p> <p>ASP: Controller</p> <p>Operates marketing campaigns</p>	<p>ASP data: company name, employee name, user ID, address, email, telephone</p> <p>ISP data: company name, contact details, employee names, email, order details (date of order, parts/services ordered, order quantity, sales, orders not placed (lost sales), frequency of use of B2B Connect Platform/aftersales related Services, further lead related information</p>

### 3. Recipients

Restricted individuals with dedicated roles to whom Personal Data will only be disclosed on a need-to-know-basis as required in order to carrying out their respective managerial responsibilities (e.g. contractors, including those for HR, IT and finance (where appropriate)); group entities, consultants, auditors, accountants; financial organisations; law enforcement agencies, government agencies, regulatory authorities.

**Mercedes-Benz-internal use only-draft**  
**Review by local legal counsel required**

**Annex 2: Technical and Organisational Measures**

The following technical and organizational measures reflect the measures implemented in the individual functional components of the relevant environment. Depending on the sub-function and application, not all of the measures indicated below may be fully implemented (e.g. special access control measures for applications that are already operated in specially protected environments, such as specially protected data centers). Specific detailed descriptions of the technical and organisational measures taken for each product component, sub-function or (partial) application will be made available on request.

See Annex 2 (sub-Annex 2) to Part A



Mercedes-Benz-internal use only-draft  
Review by local legal counsel required

**Annex 3: Subprocessors**

#	<i>Subprocessor to MB X including address / location</i>	<i>Subject matter and nature of the processing</i>	<i>Duration</i>
1.	Mercedes-Benz Group AG	Technical operation of B2B Platforms + providing user support	During the term ASP makes use of B2B Platform

\*\*\*