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

These Terms of Use are between:

(1) Mercedes-Benz UK Limited (Company No. 2448457) whose registered office is at Tongwell, Milton Keynes, MK15 8BA ("**MBUK**"); and

(2) the authorized service partner (hereinafter referred to as "**Partner**") of MBUK 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**").

MBUK and Partner are hereinafter also referred to as "**Parties**".

Preamble

B2B Connect is provided by MBUK. 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 the WebParts Dealer Client (also after migration to 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 MBUK in cooperation with MBAG. Otherwise, there is a limited availability of information.

§ 2 MBUK Services, Conclusion of contracts, Change, Participation and 5*Rater

MBUK 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 MBUK provided B2B Connect Seller Center and WebParts Dealer Clientenables 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 MBUK 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 the 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, MBUK neither assumes any warranty for performance of contracts made between Partner and Customers via B2B Connect. MBUK shall bear no duty whatsoever to ensure performance of the contracts which have been formed between Partner and Customers.

MBUK is entitled to change the functions provided through B2B Connectif such a change would not require a change to these Terms of Use. MBUK shall notify Partner in writing (e.g. email) at least one month prior to such change unless otherwise agreed.

Unless otherwise agreed MBUK 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, MBUK shall notify Partner in writing at least six (6) weeks prior to such a change. If Partner does not object to such changes in writing 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. MBUK 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, MBUK shall have the right to terminate the Partner's use of the services affected by such a change for cause.

In case that MBUK integrates 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 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 MBUK. Partner shall have the option to propose a cure within a reasonable period of time required by MBUK. If a solution proposed by Partner is not reasonably acceptable for MBUK, MBUK 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, 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 MBUK 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 MBUK) and shall be solely provided in Partner's own responsibility and relationship towards Customer and without MBUK 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 MBUK.
These 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 MBUK 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 MBUK for the performance of these Terms of Use and will be anonymized by Mercedes-Benz AG for the development of the platform.

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 MBUK 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 on B2B Connect, the Parties intend to exchange the relevant personal data among independent controllers, whereas MBUK 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 MBUK, 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, MBUK 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*Rater, 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.

MBUK 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 MBUK 1st and 2nd level support for WebParts Dealer Client. MBUK excludes any liability for the misuse of user ID and password in the Partner´s organizational unit and his Customers.

MBUK 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 MBUK 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.

In any case, the Mercedes-Benz Platform Rules as provided together with these Terms of Use as **Appendix 2** shall apply.

§ 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 MBUK. 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 MBUK or on those of service providers, which are necessary in order to ensure that B2B Connect is properly provided or improved.

§ 9 Liability, Indemnification

Nothing in these Terms of Use limits any liability which cannot legally be limited, including, but not limited to, liability for death or personal injury caused by negligence and fraud.

Liability of MBUK is limited whether in contract, tort (including negligence), breach of statutory duty, or otherwise, to direct losses only. MBUK shall not be liable to the Partner, whether in contract, tort (including negligence), breach of statutory duty, or otherwise for loss of profit, loss of business, loss of use or corruption of software, loss of or damage to goodwill and indirect or consequential loss.

In any event, MBUK's total liability to the Partner whether in contract, tort (including negligence), breach of statutory duty, or otherwise shall not exceed £5,000.

Should the Partner breach any obligation whether in contract, tort (including negligence), breach of statutory duty, or otherwise, the Partner shall indemnify MBUK for any and all damages, losses, liabilities, claims (including third party claims) and costs (including the appropriate legal fees and costs) arising from a 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 1st December 2021.

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: MBUK rights to provide WebParts Dealer Client and B2B Connect Seller Center to Partner derive from an agreement between MBAG and MBUK. MBUK 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 MBUK is liable to pay taxes and customs duties duly allocable to the sale of products posted on 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 MBUK arising from such taxes and customs duties. The same applies to value added tax owed and not paid by the Partner, for which MBUK was held liable.

§12 Place of Jurisdiction

These Terms of Use shall be governed and construed and have effect in all respects in accordance with English Law. The courts of England shall have exclusive jurisdiction over any proceedings arising out of or in connection with the Terms of Use or its subject matter or formation.

§13 Miscellaneous

MBUK may vary or amend these Terms of Use without notice to the Partner from time to time. Should the Partner determine that it does not wish to continue to use the Online Parts Trading Systems following any such variation, the Partners only remedy shall be to terminate these Terms of Use in accordance with section 9 and to cease use of the Online Parts Trading System.

All changes and additions to this agreement requested by the Partner shall only be effective with the written consent of MBUK.

These Terms of Use may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

Transmission by email of the executed signature page of a counterpart of these Terms of Use along with the final form of the agreement (in each case in PDF, JPEG, or any other agreed format) shall take effect as the transmission of an executed “wet-ink” counterpart of this agreement. Without prejudice to the validity of any agreement thus made, each party shall on request provide the other with the "wet ink" hard copy original of their counterpart.

No counterpart shall be effective until each party has executed at least one counterpart.

Appendices to these Terms of Use

Appendix 1 – Data Protection Agreement
Appendix 2 – Platform Rules

Appendix 1:

Data Protection Agreement

B2B Connect Platform and related Services

between

Mercedes-Benz UK Limited (Company No. 2448457) whose registered office is at Tongwell, Milton Keynes, MK15 8BA ("MBUK"); and

Authorized Service Partner

("ASP")

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

BACKGROUND

(A) *Whereas*, MBUKis 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 MBUKto 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", "sub-processor", "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 local data protection laws applicable in a Member State, or any other applicable data protection law as applicable to each of the Parties – jointly or separately - when performing or making use of the Services. 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 da-ta 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 Ar-ticle 28 of the GDPR.

(f) "MBAG" means Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Germany.

(g) "MB UK" means Mercedes-Benz UK Limited (Company No. 2448457) whose registered office is at Tongwell, Milton Keynes, MK15 8BA.

(h) "Clauses" shall mean, collectively, the Clauses on Data Processing on behalf of a Control-ler 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 MBUK 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) or Processor in relation to the relevant Personal Data processed as further defined in the Annexes to Parts A and B.

2.2 As the Parties wish to ensure an adequate level of protection in connection with the processing of Personal Data with respect to the protection of privacy and fundamental rights and freedoms of the data subjects, the principles set forth in Part A shall apply to any processing be-tween Controllers as described therein, notwithstanding if deemed a processing in a Joint Controllership or not.

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 MBAG and MBUK'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 writing.

6. ASSIGNMENT

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

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

This Agreement shall be governed and construed and have effect in all respects in accordance with English Law. The courts of England shall have exclusive jurisdiction over any proceedings arising out of or in connection with this Agreement or its subject matter or formation.

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.

Mercedes Benz AG

Stuttgart,

Mercedes-Benz UK Limited:

_____

[name] Sally Davies
[function] Customer Services Director

[name] Tracy Christman
[function] Head of Sales - Customer Services

Simon Neill
Signed by: Simon Neill
EMail: simon.neill@mercedes-benz.com
Signing time: 24-05-2024 11:00:06 (+01:00)
IP address: 163.116.162.118

[name]
[function]

Georgiana Simbotin
Signed by: Georgiana Simbotin
EMail: georgiana.simbotin@mercedes-benz.com
Signing time: 22-05-2024 10:53:24 (+01:00)
IP address: 163.116.162.123

[name]
[function]

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

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.

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 MBUK has been authorized by MBAG to execute these Joint-Controller Clauses 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 below, MBAG shall not become a Party to this Agreement in this respect. ASP herewith confirms and consents to MBAG becoming a Party hereunder 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 MBUK 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.	MBUK: Controller 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 ASP: Controller Supports ticket / request for ISP in collaboration with ISP; is responsible for properly handling information provided and correct processing	ISP data: ISP company name, user name, user ID, address, email, telephone, ticket or request details (date, subject) ASP data: company name, user name, user ID, address, email, telephone
Business Analytics	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, MBUK and ASP. Reports are usually created by automated calculations (application based). In exceptional cases the data is merged with data from other sources (e.g. another database from another MBAG department) to run further analysis. MBAG and its employees operate strictly according to the need-to-know principle.	MBAG: Controller Operates business logic and hosts data base with business data, creates aggregated evaluations/reports based on the provided data for itself, MBUK and ASP. MBUK: Controller Allows transmission of B2B platform transaction related data to be used for the above processes; receives aggregated reports ASP: Controller Allows transmission of B2B platform transaction related data to be used for the above processes; receives aggregated reports	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) ASP data: company name, user name, user ID, address, email, telephone

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.

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, whereas Processor will be responsible for compliace with statutory provisions on data protection that apply to a processor.

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 representativ 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 MBUK" which can be contacted via Data Protection Coordinator

Legal Department Tongwell
Milton Keynes
MK15 8BA
Email: datacompliance@daimler.com

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 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 in accordance with Art. 28 para. 3 lit. f GDPR 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 without undue delay 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 in accordance with Art. 28 para. 3 lit. e GDPR by appropriate technical and organisational measures, insofar as this is possible and reasonable, for the fulfilment of the Controller's obligation towards data subjects, (including pursuant to Chapter II of the GDPR) 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 in accordance with Art. 28 para. 3 lit. f GDPR with the preparation of a data protection impact assessment pursuant to Art. 35 GDPR and, where appropriate, assists with the prior consultation of the supervisory authority pursuant to Art. 36 GDPR. 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 MBUK which MBUK 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

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 appropriate 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.

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 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 As a general rule, the processing shall occur in a member state of the European Union, in a country of the European Economic Area or in an Adequate Country. Processing activities in another country ("Third Country") shall be allowed if the applicable requirements for international transfer of Personal Data are complied with.

10.2 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.

10.3 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.

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)	MBUK: Processor (MBAG: Subprocessor) Provides support to ASPs respectively ASP: Controller Use WebParts including user support	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	MBUK: Processor (MBAG: Subprocessor) Displays ISP transaction data in the B2B Connect Seller Center, and provides reports and analytics upon request of ASP ASP: Controller Use WebParts including data display, reporting and analytics	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 ASP data: company name, user name, user ID
Campaign Proposal Services (in case that such a service is requested by MBUK and/or ASP; otherwise not applicable)	MBAG and MBUK (if applicable) use provided data to run business analytics and creation of related marketing campaigns for MBUK 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 MBUKor 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 MBUKor ASPs for this purpose.	MBAG: Processor Hosts data base with business analytics data; operates applications and creates marketing campaigns based on the provided data for MBUK and ASPs to enable them to contact ISPs via different direct marketing channels. Transmits marketing materials + ISP lists to MBUKand/or ASPs for this purpose. MBUK: Controller Receive ISP lists + marketing materials for marketing campaigns (marketing campaigns will be operated by MBUKin its sole responsibility, if applicable) May provide similar services to ASPs (in this case acting as a processor to ASPs as well) ASP: Controller	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 WebParts/ aftersales related Services, delivery times) ASP data: company name, user name, user ID, address, email, telephone

		Receive ISP lists + marketing materials for marketing campaigns (marketing campaigns will be operated by the ASP in its sole responsibility)	
Direct Marketing Campaign Services (in case that such a service is requested by ASP; otherwise not applicable)	Optionally when ordered by an ASP MBUK 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 MBUK 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.	MBUK: Processor MBUK 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, MBUK will provide an interface via which ASP may transmit end-customer data (names, email-address) to MBUK. MBUK will then process the data transmitted for sending out of marketing emails (also via third party service providers of MBUK). Optionally, MBUK may contact ISPs through MB callcenter and follow up on prior business transactions. ASP: Controller Operates marketing campaings	ASP data: company name, employee name, user ID, address, email, telephone 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

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.

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.

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	☒	☐	☐
Specification of authorized persons, including scope of authority regarding physical access to relevant rooms or areas	☒	☐	☐
Admittance authorization IDs issued	☒	☐	☐
Rules and regulations for visitors in place	☒	☐	☐
Rules and regulations governing keys implemented	☒	☐	☐
All individuals recorded in and out	☒	☐	☐
Physical protection of company premises (e.g. fence, external walls, checkpoints)	☒	☐	☐
Secure entrance (e.g. locking system, ID readers)	☒	☐	☐
Burglar-resistant windows	☒	☐	☐
Surveillance installation (e.g. alarm system, CCTV)	☒	☐	☐
Separation system (e.g. turnstiles, double-door system)	☒	☐	☐
Documentation of physical protection measures	☒	☐	☐

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

3. Access control (user rights)	Yes	No	Not applicable
Authorization and roles concept implemented for applications	☒	☐	☐
User accounts required for data access	☒	☐	☐
Regular review of authorizations	☐	☒	☐

Access restrictions imposed (based on principles of need-to-know and least privilege)	☒	☐	☐
Additional passwords (based on the 4-eyes-principle) for particularly important functions (e.g. system admin)	☒	☐	☐
Securing of multi-client capability of the system	☒	☐	☐
Separated and multi-client capable databases	☒	☐	☐
Separation of development, test, integration and productive environment	☒	☐	☐
Separation of productive and archiving environment	☒	☐	☐
Read-access logged	☒	☐	☐
Write-access logged	☒	☐	☐
Unauthorized access attempts logged	☒	☐	☐
Implementation of retention periods for data	☒	☐	☐

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

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

6. Job control	Yes	No	Not applicable
Daimler‘s standard agreement on data processing on behalf has been agreed on	☒	☐	☐
Data processor’s standard agreement on data processing on behalf has been agreed on	☒	☐	☐
Standard Contractual Clauses of the EU Commission has been agreed on for data processing on behalf by processors in third countries	☒	☐	☐
Responsibilities of data controller and data processor are strictly regulated / separated	☒	☐	☐
Rules specified to adjust / change instructions given to the data processor	☒	☐	☐
On-site controls have been conducted and documented by the data controller	☐	☒	☐

Data processor submitted self-assessments	☐	☒	☐
Data processor submitted approved certifications	☐	☒	☐
Data processor submitted list of subcontractors	☒	☐	☐
Checks on subcontractors by processor	☐	☒	☐

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

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)	☒	☐	☐
Revision of the implementation of the described measures	☒	☐	☐
Description of applicable data protection requirements in binding guidelines and instructions for action	☒	☐	☐
Involvement of the data protection officer in relevant new data processing procedures	☒	☐	☐

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	☒	☐	☐
Specification of authorized persons, including scope of authority regarding physical access to relevant rooms or areas	☒	☐	☐
Admittance authorization IDs issued	☒	☐	☐
Rules and regulations for visitors in place	☒	☐	☐
Rules and regulations governing keys implemented	☒	☐	☐
All individuals recorded in and out	☒	☐	☐
Physical protection of company premises (e.g. fence, external walls, checkpoints)	☒	☐	☐
Secure entrance (e.g. locking system, ID readers)	☒	☐	☐
Burglar-resistant windows	☐	☐	☒
Surveillance installation (e.g. alarm system, CCTV)	☒	☐	☐
Separation system (e.g. turnstiles, double-door system)	☒	☐	☐
Documentation of physical protection measures	☒	☐	☐

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

3. Access control (user rights)	Yes	No	Not applicable
Authorization and roles concept implemented for applications	☒	☐	☐
User accounts required for data access	☒	☐	☐
Regular review of authorizations	☒	☐	☐
Access restrictions imposed (based on principles of need-to-know and least privilege)	☒	☐	☐
Additional passwords (based on the 4-eyes-principle) for particularly important functions (e.g. system admin)	☐	☒	☐
Securing of multi-client capability of the system	☒	☐	☐
Separated and multi-client capable databases	☐	☒	☐

Separation of development, test, integration and productive environment	☒	☐	☐
Separation of productive and archiving environment	☒	☐	☐
Read-access logged	☒	☐	☐
Write-access logged	☒	☐	☐
Unauthorized access attempts logged	☐	☐	☒
Implementation of retention periods for data	☐	☒	☐

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

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

6. Job control	Yes	No	Not applicable
Daimler‘s standard agreement on data processing on behalf has been agreed on	☐	☒	☐
Data processor’s standard agreement on data processing on behalf has been agreed on	☐	☒	☐
Standard Contractual Clauses of the EU Commission has been agreed on for data processing on behalf by processors in third countries	☐	☒	☐
Responsibilities of data controller and data processor are strictly regulated / separated	☒	☐	☐
Rules specified to adjust / change instructions given to the data processor	☒	☐	☐
On-site controls have been conducted and documented by the data controller	☐	☒	☐
Data processor submitted self-assessments	☐	☒	☐
Data processor submitted approved certifications	☐	☒	☐
Data processor submitted list of subcontractors	☒	☐	☐
Checks on subcontractors by processor	☐	☐	☒

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

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)	☒	☐	☐
Revision of the implementation of the described measures	☒	☐	☐
Description of applicable data protection requirements in binding guidelines and instructions for action	☒	☐	☐
Involvement of the data protection officer in relevant new data processing procedures	☒	☐	☐

Annex 3: Subprocessors

#	*Subprocesor to MBUKincluding address / location*	*Subject matter and nature of the processing*	*Duration*
1.	*Mercedes Benz Group AG*	*Technical operation of B2B Platform + providing user support*	*During the term ASP makes use of B2B*

Appendix 2: Platform Rules

1. General Platform Rules

MBUK reserves the right to block Partners or Customers (hereinafter together also referred to as "Users" or "User") or take other appropriate measures in the event of signs of improper use of B2B Connect or use that violates the applicable contractual provisions. In particular, such use shall be deemed to be improper if User uses B2B Connect or information provided therein for purposes other than those for which they were intended, uses it for purposes that are illegal or violate the rights of MBUK or third parties, or uses B2B Connect in non-compliance with other guidelines provided by MBUK.

User warrants that all information provided to MBUK and other Users will be true, accurate and complete at all times and in compliance with all legal requirements and applicable contractual provisions. User undertakes to inform MBUK without delay of any future material changes to the information provided to MBUK that are relevant to the contractual or usage relationship.

In particular, B2B Connect may not be used for the dissemination of information that meets the following criteria: racist, inhuman slogans; the provision of false or otherwise incorrect information; information that is offensive, abusive, harassing, hateful, obscene, threatening or otherwise objectionable; information that violates legal requirements or with which applicable requirements are not sufficiently observed or implemented (e.g. in the case of labelling or transparency obligations); information whose provision or dissemination constitutes a criminal offence or misdemeanor; information the provision or dissemination of which constitutes a criminal offence or an administrative offence.

If information provided violates the applicable terms of use of B2B Connect and MBUK becomes aware of it (e.g. through a report from a Customer or other third party), MBUK reserves the right to immediately (if necessary also only temporarily) block or delete the corresponding content and to take all further necessary steps.

If necessary or appropriate, the following measures will be taken depending on the severity, frequency and number of the violation(s):

- temporary or permanent deletion of content;
- temporary blocking of a User account or User access;
- inactivation of the User account or User access for 3 months;
- permanent blocking of the User account and all associated content;
- permanent blocking of the User account and all associated content and inclusion of the access data, in particular the specified e-mail address and other master data for identifying User, on a blacklist with the consequence that a new User account or content cannot be created;

To the extent legally required, User will be informed of MBUK's decision and given the opportunity to comment. After further commenting (or in the absence of any such comments), MBUK will reconsider the decision and make a final decision on how to handle the affected content. Depending on the case, additional moderation measures as described in the relevant terms of use for B2B Connect will be applied. User will receive a notification/email about the moderation decision made, including a justification.

Comments or request regarding a moderation decision under Digital Services Act can be directed to the contact points listed in section 3.2. User needs to specify which decision he/she is referring to (e.g. by stating the date, subject and/or file number) and what he/she objects to about the decision or would like to have explained in more detail.

Complaints that cannot be resolved through the processes described above can be submitted to and processed by a certified out-of-court dispute resolution body. Where necessary, information regarding access to an out-of-court dispute resolution body will be made available at the B2B website under "legal notice". Irrespective of the involvement of such a body, recourse to the competent courts is always possible.

2. Identification of commercial and advertising content

Where Users provide information to other Users within B2B Connect, it must indicate commercial offers and advertising in accordance with applicable laws.

In the context of advertising offers, Users must provide transparent information about the advertiser. This includes, for example, in whose name the advertisement is displayed and who has paid for the advertisement.

If advertising offers are displayed to different Users or User groups depending on the User or User group behavior or the like (in particular in case of targeting or profiling), User must provide transparent information about the relevant parameters for determining the information to be displayed to other Users or User groups. User must keep all information up to date at all times.

MBUK will, as far as possible, provide technical measures and possibilities within B2B Connect with which User can fulfill the corresponding obligations. Should no such measures be provided or should these measures not be sufficient from the User's point of view, it shall immediately inform MBUK of it and the Parties will immediately coordinate the implementation of corresponding measures.

3. Contact points

For inquiries about content on B2B Connect, User can use the contact points that he/she can find on the B2B website under "Provider / Data privacy". When contacting MBUK, User should always specify his/her inquiry by stating what his/her inquiry refers to, why User contacts MBUK in this regard and how MBUK may help User with his/her inquiry.

3.1 Illegal contents

If User wishes to report illegal content and violations of the applicable terms of use of B2B Connect, User can refer to the contact form as provided at the B2B website under "Provider / Data privacy". When contacting MBUK, User should always specify his/her inquiry by stating e.g. why User believes a certain content is illegal or violates certain regulations, where such content can be found, when User found it etc.).

3.2 Complaints and questions against a decision

If User wishes to contact MBUK with a complaint against a decision made against him/her as described above, User should refer to the contact form as provided at the B2B website under "Provider / Data privacy".

***