General Terms and Conditions for Continental Automotive Edge Framework ("CAEdge")

10. SCOPE OF THE GENERAL TERMS AND CONDITIONS, PARTS OF THE CONTRACT

10.1 Continental Automotive Technologies GmbH, having its registered place of business at Continental-Plaza 1, 30175 Hanover, Germany ("**CONTINENTAL**") provides CAEdge™ and the associated services as further defined hereafter (together the "**SERVICE**") exclusively based on the following General Terms and Conditions (hereinafter, the "**GENERAL T&C's**"). The GENERAL T&C's and the following documents constitute the contractual basis for the provision of the SERVICE ("**AGREEMENT**")

- SERVICE specific terms ("**SERVICE SPECIFIC TERMS**")
- CUSTOMER's order and CONTINENTAL's order confirmation for the SERVICE
- Service description of the SERVICE ("**SERVICE DESCRIPTION**")
- Data Processing Agreement ("**DPA**")

These GENERAL T&C´s including the further documents mentioned above apply only to the SERVICE and not to other services from CONTINENTAL.

10.2 If there are any inconsistencies between the documents mentioned in **Section 10.1** of this AGREEMENT, the order of priority shall be as follows – exempt where otherwise expressly stated in this AGREEMENT: (i) CONTINENTAL's order confirmation; (ii) CUSTOMER's order; (iii) the SERVICE SPECIFIC TERMS (iv) the GENERAL T&C's; (iv) the SERVICE DESCRIPTION, (v) the DPA. Other documents referenced by this AGREEMENT are on the same level of precedence as the part of the AGREEMENT in which they are referenced.

For the avoidance of doubts, the DPA shall take precedence over all other contractual documents mentioned in this Section 10 as far as mandatory data protection requirements are affected.

10.3 General terms and conditions of the CUSTOMER are not accepted. This shall also apply if a reference is made to the applicability of the CUSTOMER's general terms and conditions in the CUSTOMER's order, registration or in other documents and CONTINENTAL does not expressly object to this.

11. NON-BINDING NATURE OF ADVERTISING STATEMENTS, CONTRACT CONCLUSION

11.1 Offers, statements and/or information made and/or given by CONTINENTAL in brochures, advertisements and similar items – also with regard to prices – are and remain non-binding and subject to changes without notice, unless a binding, specific offer and/or commitment has expressly been made.

11.2 The contract with the CUSTOMER regarding the SERVICE shall enter into effect when the respective order of the CUSTOMER has been explicitly accepted by CONTINENTAL by way of an electronic contract conclusion, by an explicit order confirmation of CONTINENTAL and/or a written document properly signed by both contractual Parties, but at the latest with the first use of the SERVICE by the CUSTOMER and/or its users.

12. PROVISION OF THE SERVICE

12.1 The subject of the AGREEMENT is the provision of CAEdge, CONTINENTAL's Automotive Edge Framework for development and management of automotive software, against payment for the usage by the CUSTOMER as Software as a Service (SaaS) and/or Platform as a Service (PaaS). Further details can be found in the SERVICE DESCRIPTION.

12.2 CONTINENTAL provides the CUSTOMER with the SERVICE subject to this AGREEMENT and within the scope of its actual availability. CUSTOMER is aware that malfunctions and failures may occur in the operation of the SERVICE, during which access is temporarily hindered or excluded. CONTINENTAL will endeavor to keep the SERVICE operational and the maintenance-related unavailability low.

12.3 Data connection between the CUSTOMER's IT infrastructure and the SERVICE (e. g. via internet) are not subject of this AGREEMENT and are not provided by CONTINENTAL (see also **Section 14.4** below). Solely the CUSTOMER and/or the user are responsible for that.

12.4 CONTINENTAL is not obliged to provide the SERVICE on own servers or own storage space. CONTINENTAL is authorized to commission third-party service providers or subcontractors including cloud providers or cloud services.

12.5 CONTINENTAL may monitor the usage activities of the CUSTOMER and its users to the extent permitted by law to ensure safe and stable operation of the SERVICE. If CONTINENTAL makes the

API for the SERVICE available to the CUSTOMER, it shall only be used for the purpose of using the SERVICE and in accordance with the AGREEMENT. CONTINENTAL reserves the right to monitor the use of the API and restrict or throttle the CUSTOMER's API access either temporarily or permanently, e.g. to ensure all users receive the same service quality or in case of detected misuse or abnormal activity.

12.6 CONTINENTAL may temporarily or permanently restrict or block CUSTOMER's and/or individual user's access to the SERVICE if there are reasonable indications that the CUSTOMER or its users are violating or have violated any term(s) of this AGREEMENT and/or the applicable law, or if the security of the SERVICE or the systems used to operate the SERVICE are affected.

12.7 CONTINENTAL is not obligated to support nor maintain prior versions of the SERVICE.

12.8 CONTINENTAL may utilize and/or make available third-party products, services or functionalities in the provision of the SERVICE and for creating or processing of CUSTOMER CONTENT ("**THIRD-PARTY SERVICE**"). The access and use of such THIRD-PARTY SERVICE may be subject to the specific terms and conditions of the respective THIRD-PARTY SERVICE provider as made available to CUSTOMER within the SERVICE. CONTINENTAL is not responsible and liable for any THIRD-PARTY SERVICE (including without limitation, the content made available via the THIRD-PARTY SERVICE, its functionality, uptime, outages or malfunctions and failures). Any use of THIRD-PARTY SERVICE is on CUSTOMER's own risk and account.

13. USER ACCOUNTS

13.1 In order to make use of the SERVICE, CUSTOMER may register its employees as users for the SERVICE on the basis of a named user license model. The registration of virtual or technical users (e.g. by implementation of scripts) is prohibited.

13.2 The CUSTOMER must truthfully and accurately provide the information requested during registration. Registration takes place in particular by providing the following information:

13.2.1 CUSTOMER information (i.e. company, legal form, registered address, contact person)

13.2.2 Name, function and business e-mail of the users to be created

13.2.3 Project ID, to which user shall be onboarded, if any

(collectively, "**REGISTRATION DATA**").

13.3 CONTINENTAL reserves the right to refuse the opening of the user account after verifying the REGISTRATION DATA. The user account is only opened with express confirmation by CONTINENTAL or by transmission of the access data to the concerned user or to the CUSTOMER.

13.4 If the prerequisite for using the Service is met, CONTINENTAL will open the requested user accounts for CUSTOMER. The user accounts are not transferable and may only be used by the specified users.

13.5 CONTINENTAL shall provide CUSTOMER's users with the data and identifications (username, password) required to access the SERVICE ("**ACCESS DATA**") via the e-mail addresses provided.

13.6 The administration of the user accounts is carried out by CONTINENTAL.

13.7 After a period of more than 6 months of inactivity, CONTINENTAL may delete user accounts with reasonable notice.

13.8 CUSTOMER must inform CONTINENTAL immediately of any changes to the REGISTRATION DATA associated with the respective user account (e.g. departure of the user from the CUSTOMER, entry of new users).

13.9 The ACCESS DATA must be kept secret and protected against access by unauthorized third parties. CONTINENTAL must be informed immediately of any loss and/or disclosure of access data to third parties. If CONTINENTAL detects misuse or any abnormal activity, or if CONTINENTAL reasonably beliefs that ACCESS DATA is compromised, or that CUSTOMER's user violates any terms of this AGREEMENT, CONTINENTAL is entitled to revoke the ACCESS DATA.

14. RIGHTS OF USAGE

14.1 Limited to the term of the SERVICE, CONTINENTAL grants the CUSTOMER a non-exclusive, non-transferable, non-sublicensable, revocable right to access and to make use of the SERVICE as specified in the SERVICE DESCRIPTION. If CONTINENTAL provides new versions, updates, upgrades etc. during the term of this AGREEMENT, the above rights shall apply respectively.

14.2 Source code will not be provided, except as expressly stated in the SERVICE DESCRIPTION.

14.3 CONTINENTAL retains all rights, title and interest in and to the SERVICE. No ownership rights are being conveyed to CUSTOMER or its users under this AGREEMENT. Except for the express rights

granted herein, CONTINENTAL does not grant any other licenses or access, whether express or implied, to any CONTINENTAL software, services, technology or intellectual property rights.

14.4 CUSTOMER acknowledges that the SERVICE may contain open source or third-party components. For the avoidance of doubt, all utilization of such components is governed by the applicable open source or third-party licenses, as detailed in the accompanying documentation.

15. DUTIES AND RESPONSIBILITES OF THE CUSTOMER

15.1 The CUSTOMER is obliged to ensure that the hardware and/or software used by it, including computers, routers, tablets etc., are in line with the common state-of-the-art and will be maintained and/or updated regularly in accordance with the recommendations of the respective manufacturers; any technical specifications and/or minimum requirements for the SERVICE published by CONTINENTAL shall be complied with.

15.2 The CUSTOMER grants CONTINENTAL the right to reproduce the data stored by the CUSTOMER using the SERVICE to the extent necessary to render the services to be provided under this AGREEMENT. In order to correct problems, CONTINENTAL is also authorized to make changes in the structure or the data format.

15.3 CUSTOMER may only enable third parties to use the SERVICE with the prior consent of CONTINENTAL in text form (§ 126 b BGB). Allowing third parties to use the SERVICE on a commercial basis is expressly prohibited. CUSTOMER must take precautions against unauthorized access by third parties to the SERVICE as well as against unauthorized use of any user manual.

15.4 CUSTOMER will not (and will not allow any third party to): (i) use, resell, sublicense, rent, lease, assign or share the SERVICE, or any component thereof, with or for any third party, or (ii) gain or attempt to gain unauthorized access to the SERVICE or any element thereof, circumvent or otherwise interfere with any authentication or security measures of the SERVICE, or permit or gain unauthorized access to the SERVICE; or (iii) interfere with or disrupt the integrity or performance of the SERVICE, or (iv) use automated methods (in particular data mining) to access data from the SERVICE, transmit material containing software viruses, malware or other harmful or deleterious computer code, files, scripts, agents, or program through or into the SERVICE or in any other way attempt to circumvent or interfere with the proper functioning, integrity, operation or appearance of the SERVICE and the systems used for it; or (v) decompile, disassemble, scan, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of the SERVICE (except to the extent that applicable law expressly prohibits such a reverse engineering restriction); or (vi) provide, lease, lend, sublicense, use for timesharing or service bureau purposes or otherwise use or allow others to use the SERVICE or any component thereof for the benefit of any third party; or (vii) perform benchmark tests on the SERVICE; or (viii) use, evaluate or view the SERVICE for the purpose of designing, modifying or otherwise creating any environment, software, models, algorithms, products, program or infrastructure or any portion thereof, which performs functions similar to the functions performed by the SERVICE.

15.5 The CUSTOMER is obliged to maintain confidentiality towards third parties with regard to any ACCESS DATA provided by CONTINENTAL and to secure them against any unauthorized access so that any misuse by third parties is excluded. Passwords should be changed at regular intervals. CONTINENTAL must be notified without undue delay about any loss and/or disclosure of any ACCESS DATA to third parties. CONTINENTAL reserves the right to block the access to the SERVICE if there is reasonable suspicion of misuse of the ACCESS DATA by third parties. If necessary, CONTINENTAL assigns a new user identification to the CUSTOMER.

15.6 The CUSTOMER will immediately inform CONTINENTAL of any change in his company name, place of residence or business or legal form without undue delay.

15.7 CUSTOMER shall procure that its users comply with this AGREEMENT and the ACCEPTABLE USE POLICY attached to this GENERAL T&Cs and as made available within the SERVICE. CUSTOMER is responsible for all actions and omissions of CUSTOMER's users, whether authorized or unauthorized. CUSTOMER undertakes not to and ensures that users do not use the SERVICE for any illegal purpose; or use the SERVICE in violation of the ACCEPTABLE USE POLICY; or send any illegal or harmful data to or via the SERVICE, create a security vulnerability to the SERVICE or otherwise interfere with or disrupt the SERVICE or the servers or networks providing the SERVICE ("**PROHIBITED USE**").

16. MAINTENANCE & MONITORING

16.1 CONTINENTAL undertakes to provide constant care and maintenance of the SERVICE in accordance with the following provisions.

16.2 CONTINENTAL is entitled to replace previous versions of the SERVICE with newly developed versions at any time, in particular, if this is necessary, to adapt the SERVICE to changed legal requirements and/or standards or to adapt it to technical or scientific knowledge; **Section 19** shall

apply accordingly. In the case of third-party software and/or services, CONTINENTAL shall proceed accordingly as far as the developer of the software has provided a new development or adaptation to CONTINENTAL.

16.3 CONTINENTAL undertakes to monitor and maintain the SERVICE. The CUSTOMER shall be informed of any errors or malfunctions, which not only insignificantly impair or limit the use of the SERVICE in due time; whether warranty and/or defect claims exist in that relation is subject to **Section 21**.

17. DATA USAGE

In order to provide the SERVICE CONTINENTAL needs to track, monitor, collect, share, store and process data of the CUSTOMER and its users collected when using the SERVICE ("**USAGE DATA**"). CUSTOMER acknowledges and agrees that CONTINENTAL may collect USAGE DATA and analyse, use and disclose such USAGE DATA in an aggregated format to monitor the security of the SERVICE, identify and address technical problems and to improve the SERVICE or otherwise pursue CONTINENTAL's business purposes; provided the aggregated USAGE DATA does not include personally identifiable information and does not include confidential information of CUSTOMER or CUSTOMER CONTENT.

18. PAYMENT TERMS, EXCLUSION OF OBJECTIONS

18.1 Invoices for fees of SERVICE are due for payment within two (2) weeks of receipt. The CUSTOMER may issue a direct debit authorization to CONTINENTAL in order to simplify payments and/or use other payment methods accepted by CONTINENTAL.

18.2 All fees are exclusive of value added tax (VAT).

18.3 If the CUSTOMER is in default of payment for more than thirty (30) days, CONTINENTAL reserves the right to suspend the CUSTOMER's access to the SERVICE after a written demand for payment and the futile expiry of a reasonable grace period. In this case, the CUSTOMER remains obliged to pay the agreed fees in full when due.

18.4 The CUSTOMER must raise objections against invoices without undue delay in text form (§ 126 b BGB, e. g. letter, email), at the latest within a period of six weeks after their receipt. Failure to raise objections in due time shall be deemed as acceptance of the respective invoice. CONTINENTAL will expressly inform the CUSTOMER of the consequences of failing to observe the prescribed deadline before the beginning of the respective objection period (e.g. within the invoices).

19. CHANGES

19.1 CONTINENTAL is entitled to modify the SERVICE at any time if such modifications are in favor of the CUSTOMER and the contractual terms and conditions as well as the fees remain unchanged. Furthermore, changes to the SERVICE are permissible as far as this is objectively reasonable for the CUSTOMER and the contractually agreed performances will not be significantly changed; this may in particular include technical improvements and innovations as well as changes for legal, technical, operational or security reasons. Material changes to the SERVICE will be notified to the CUSTOMER within reasonable time in advance. If a change in the SERVICE affects the essential interests of the CUSTOMER in such a way that it is no longer reasonable to the CUSTOMER to adhere to the AGREEMENT, the CUSTOMER has the right to terminate the AGREEMENT within one month upon the change has come into effect and with a notice period of six (6) weeks.

19.2 CONTINENTAL reserves the right to change and amend the contractual conditions of the AGREEMENT with effect for the future. Therefore, CONTINENTAL shall inform the CUSTOMER in text form (§ 126b BGB - e. g. letter, e-mail or push/pop-up message within the SERVICE) about such changes to the AGREEMENT within reasonable time in advance, however not later than eight (8) weeks prior the changes become effective. Such changes shall be deemed accepted by the CUSTOMER, unless the CUSTOMER rejects the changes within a notice period of six (6) weeks upon receipt of the change notification. Insofar as the CUSTOMER rejects the changes in time, the contractual relationship shall continue unchanged on the basis of the current AGREEMENT including the current terms and conditions.

19.3 In the event that the CUSTOMER rejects the changes in time, CONTINENTAL is entitled to terminate the AGREEMENT by observing a notice period of three (3) months to the end of a calendar month (special termination right).

19.4 CONTINENTAL will inform the CUSTOMER about the consequences of rejecting and failing to reject in due time within the change notification.

20. TERM, TERMINATION

20.1 This AGREEMENT remains in force until terminated ("**TERM**").

20.2 The SERVICE is provided as subscription and has an initial term of one (1) year ("**INITIAL PERIOD**") and shall automatically renew for additional periods of each one (1) year ("**RENEWAL PERIOD**", collectively with INITIAL PERIOD, the "**SERVICE PERIOD**"), unless either PARTY gives the other PARTY notice of non-renewal at least thirty (30) days before the end of the then current SERVICE PERIOD.

20.3 CONTINENTAL may change the fees for any RENEWAL PERIOD by providing CUSTOMER with notice at least sixty (60) days before the end of the then current SERVICE PERIOD.

20.4 In the event that the statutory value added tax rate (VAT) changes, CONTINENTAL is entitled to adjust its remuneration accordingly, also within the current SERVICE PERIOD. In this case, the CUSTOMER has no right of termination.

20.5 CONTINENTAL may suspend or limit CUSTOMER's access to and use of the SERVICE in case (i) of PROHIBITED USE, or (ii) CUSTOMER is in breach of this AGREEMENT, or (iii) CUSTOMER acts in a manner that CONTINENTAL reasonably believes may harm CONTINENTAL, its other customers, or the SERVICE, or (iv) if required to by court order or order of another governmental authority, or (ii) CONTINENTAL reasonably determines that the SERVICE is subject to a security incident, denial of service attack, or other event that impacts the security of the SERVICE or CUSTOMER CONTENT. CONTINENTAL will use reasonable efforts to give CUSTOMER prior notice if access will be suspended and, if the issue is capable of resolution, will promptly restore access once the issue has been resolved. CONTINENTAL shall have no liability for any damage or loss as a result of any suspension, limitation or termination of CUSTOMER's access to the SERVICE pursuant to this section.

20.6 If the CUSTOMER materially breaches this AGREEMENT and does not cure such breach within thirty (30) days after receiving notice from CONTINENTAL describing such breach in reasonable detail, CONTINENTAL shall have the right to immediately terminate this AGREEMENT for cause.

20.7 CONTINENTAL can immediately terminate the SERVICE if a change in laws or regulations makes it unlawful, or impractical, in CONTINENTAL's reasonable judgment to provide the SERVICE, and CONTINENTAL, as CUSTOMER's sole and exclusive remedy, shall reimburse fees paid in advance on a pro rata basis.

20.8 CONTINENTAL may immediately terminate this AGREEMENT upon written notice to the CUSTOMER if the CUSTOMER becomes involved in and does not, within 30 days vacate, any bankruptcy, composition with creditors, liquidation (except voluntary liquidation for purpose of reorganization) or controlled administration or insolvency proceeding, or if the application for such proceeding is dismissed for lack of sufficient funds. CUSTOMER shall notify CONTINENTAL in the foregoing cases without undue delay.

20.9 Upon termination or expiry of the AGREEMENT, the SERVICE and CUSTOMER's right to access and use the SERVICE shall immediately cease. CUSTOMER may access and download it's CUSTOMER CONTENT within a grace period of 3 months after termination or expiry of the AGREEMENT. After expiry of such grace period CONTINENTAL will disable CUSTOMER's access to the SERVICE and shall not be obliged to store, archive or back-up any of CUSTOMER's CUSTOMER CONTENT and is entitled to delete it.

20.10 In case of early termination, fees paid in advance shall not be reimbursed, unless stated otherwise in this AGREEMENT.

21. WARRANTY

21.1 Each PARTY represents and warrants that (i) it has the legal power and authority to enter into and perform this AGREEMENT; and (ii) the person executing this AGREEMENT, on its behalf has the legal power and authority to do so, (iii) the SERVICE does not, to CONTINENTAL's knowledge, infringe any copyright, patent, trademark, trade secret or other intellectual property right of any third party; (v) subject to the following provisions of this **Section 21** the SERVICE will conform to descriptions as detailed in the SERVICE DESCRIPTION.

21.2 In the event of defects in the SERVICE, CONTINENTAL shall only be liable for material defects and defects of title in accordance with the statutory provisions applicable and as set out in this **Section21**. Material defect means in particular malfunctions and/or errors, which not only insignificantly impair or limit the use of the SERVICE. The remedy measures, which the CUSTOMER can claim under warranty aspects, in particular maintenance and troubleshooting, are conclusively specified in the SERVICE DESCRIPTION.

21.3 In the event CONTINENTAL breaches the above warranties, CONTINENTAL shall correct the deficiencies to cause the SERVICE to conform to the above warranties and the terms of the SERVICE DESCRIPTION. To the extent permitted under applicable law CONTINENTAL hereby disclaims all other warranties, whether express or implied, including, without limitation, the implied warranties of merchantability or fitness for a particular purpose.

21.4 In no event shall CONTINENTAL be liable for CUSTOMER CONTENT, THIRD-PARTY SERVICES made available via the SERVICE, any interception or interruption of any communications through the internet, wireless or cellular network coverage or for unavailability of or interruption or delay in telecommunications or for third parties other than those acting as CONTINENTAL's agents and subcontractors.

21.5 The CUSTOMER shall present all claims in connection with this AGREEMENT without undue delay but not later than two (2) weeks after the incident giving raise to the claim has occurred.

22. LIABILITY

22.1 Unless otherwise specified in the AGREEMENT (including the following provisions), each PARTY's liability for any violation of contractual and non-contractual obligations shall be governed by the statutory provisions.

22.2 Irrespective of the legal basis, where liability is based on fault, CONTINENTAL's liability for damages caused by intentional acts and gross negligence shall be unlimited. In the event of simple negligence, CONTINENTAL shall only be liable for:

- Damages for injury to bodily integrity, life or health; and
- Damages resulting from a breach of a material contractual obligation (i.e. an obligation the performance of which is fundamental to the due performance of the AGREEMENT and the compliance with which CUSTOMER typically relies upon and is entitled to rely upon); in this case CONTINENTAL's liability shall be limited to typical and foreseeable damages.

22.3 In any event, CONTINENTAL's maximum aggregate liability to CUSTOMER for damages resulting from breaches of material contractual obligations shall not exceed the fees paid for the SERVICE during the last year prior to the occurrence of such claim.

22.4 Liability for loss of data shall be limited to the usual restoration costs that would have been incurred if backup copies had been made regularly and at risk.

22.5 The strict liability under Sec. 536a Par. 1 of the German Civil Code is excluded.

22.6 The foregoing limitation shall not apply where CONTINENTAL has assumed a guarantee and for claims under the German Product Liability Act (*Produkthaftungsgesetz*).

22.7 All CUSTOMER claims for damages shall become time-barred within one (1) year unless a longer limitation period is required by statutory law.

23. CONFIDENTIALITY

23.1 All information, data, drawings, specifications, documentation, software listings, source and object code (other than open source) which CONTINENTAL may have imparted and may impart to CUSTOMER relating to the SERVICE ("**CONTINENTAL CONFIDENTIAL INFORMATION**") is proprietary and confidential. CUSTOMER hereby agrees that it shall keep CONTINENTAL CONFIDENTIAL INFORMATION confidential, use it solely in accordance with the provisions of this AGREEMENT and that it shall not at any time during this AGREEMENT and for a period of three (3) years after expiry or termination of this AGREEMENT, disclose CONTINENTAL CONFIDENTIAL INFORMATION, whether directly or indirectly, to any third party without CONTINENTAL's prior written consent, unless CUSTOMER is obliged to do so by statutory law, requirements of public authorities or court order. In such case disclosure shall be limited to the necessary extent and CUSTOMER shall notify CONTINENTAL as soon as possible and permissible.

23.2 Information that at the time of disclosure by CONTINENTAL (a) was generally known, (b) already in possession of or known to the CUSTOMER, (c) independently developed by CUSTOMER without use of CONTINENTAL CONFIDENTIAL INFORMATION, or (d) received by CUSTOMER from a third party without breach of any confidentiality obligation, shall not constitute CONTINENTAL CONFIDENTIAL INFORMATION.

23.3 In addition, without limiting the obligations stated in this Section 23, the applicable non-disclosure agreement(s) between the Parties, if any, are hereby incorporated by reference and shall govern the confidential information disclosed under this AGREEMENT.

24. FINAL PROVISIONS

24.1 Due to applicable (re-) Export Control regulations, items (e.g. software) can be subject to export control regulations. CUSTOMER is required to comply with all applicable export control regulations and laws prior to any export and to obtain – if necessary – licenses and/or permits. Additionally, exports (including but not limited to the provision of software via email, cloud, websites etc.) to or access from countries sanctioned according to UN and/or EU embargoes are prohibited.

24.2 This AGREEMENT constitutes the entire agreement and understanding of the Parties and supersedes any previous agreement between the Parties relating to the subject matter of this

AGREEMENT. If not provided otherwise in the GENERAL T&Cs, any changes and/or modifications to this AGREEMENT require at least text form (§ 126b BGB, e. g. letter, e-mail) to be valid.

24.3 Should a provision be invalid, unenforceable, or become invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected.

24.4 The CUSTOMER agrees that CONTINENTAL may at any time transfer its rights and obligations under this AGREEMENT in whole or in part (contract transfer) to a company affiliated with CONTINENTAL and/or CONTINENTAL AG, Continental-Plaza 1, 30175 Hanover, Germany. If such a transfer affects the legitimate interests of the CUSTOMER, the CUSTOMER may terminate the AGREEMENT without notice on the day the transfer takes effect.

24.5 Any set-off with counterclaims is permissible to the extent that the counterclaims are undisputed or have been finally adjudicated. This also applies to any right of retention.

24.6 The present AGREEMENT is exclusively governed by German law excluding its conflict of laws provisions. The application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is excluded. Place of jurisdiction for all disputes under or in connection with this contractual relationship is Hannover.

Annex 1
ACCETABLE USE POLICY (AUP) FOR CAEDGE

Acceptable Use Policy – information to the user

The user ("**User**" or "**You**") must read and acknowledge the rules outlined in this Acceptable Use Policy ("**AUP**") when using the CONTINENTAL Automotive Edge Framework (the "**SERVICE**"). Access to and use of the SERVICE are provided to the User on the basis of the corresponding service agreement between CONTINENTAL and CONTINENTAL's CUSTOMER, the company employing the User (the "**AGREEMENT**").

1. Reservation of Rights and Restrictions of use

a. CONTINENTAL and the Affiliates ("**Affiliate**" means any legal entity which is directly or indirectly controlled by Continental Aktiengesellschaft, Continental-Plaza 1, 30175 Hannover, Germany, whereby "control" means the ownership direct or indirect of more than 50 % of such legal entity's voting rights or capital) as well as any licensors of CONTINENTAL reserve any rights in their trademarks, design patents, commercial designations, titles and/or any other intellectual property but for the limited rights granted in the SERVICE. CONTINENTAL and/or any Affiliate will enforce its intellectual property rights throughout the world within the scope of the applicable legislation.

b. The use, in particular, but not limited to, the reproduction, distribution, making available to the public or adaption (if any), of any content in the SERVICE, in particular, but not limited to, any pictures, texts, data sheets, product information, graphics, animations, videos and/or other media, data, information and/or material (if any), is only permissible for the purpose as defined in the AGREEMENT. Any other use for any other purpose is not permitted without the prior written consent of CONTINENTAL, the Affiliates and/or a third-party right holder, unless permissible under the applicable law.

c. The User is not entitled to:

- Distribute, copy (unless this is for the intended use), modify or edit, adapt, translate, create derivative works from, or transform the SERVICE.
- License, transmit, commercially distribute or exploit, share or make publicly available the SERVICE, provide or rent the SERVICE to third parties.
- Extract the trademarks, product names, logos, marks and other signs ("**SIGNS**") depicted and/or used in the content and/or the SERVICE.
- Decompile, reverse engineer, disassemble, or otherwise attempt to obtain source code, object code, or underlying structural ideas, know-how, or algorithms, or other functionality of the SERVICE, except as permitted on a case-by-case basis by mandatory law.
- Remove or modify any proprietary rights, trademark rights, patent rights and other intellectual property rights notices used in the content and/or in the SERVICE in general.
- Use any device, software, or routine that interferes with any application, function, or use of the SERVICE, or is intended to damage, create undue load, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data, or communication stored or transmitted therewith.
- Circumvent or disclose the authentication or security of the User account, the underlying technology of the SERVICE or any host, network, or account related thereto.
- Use the SERVICE
    i. to store, download or transmit infringing, defamatory or otherwise unlawful or unauthorized material or malicious code or malware, or
    ii. to engage in phishing, spamming, denial-of-service attacks or other fraudulent or criminal activity;
    iii. to compromise the integrity or performance of third party systems;
    iv. to attempt to gain unauthorized access to CONTINENTAL's services, systems or networks

v. for any unauthorized (e.g., military) purposes.

d. None of the information in and/or in connection with the SERVICE is to be interpreted as granting a license to use the trademarks, design patents, commercial designations, titles and/or any other intellectual property but for the limited rights granted in the AGREEMENT. The conclusion cannot be drawn that the trademarks, design patents, commercial designations, titles and/or any other intellectual property are freely available to anyone simply from the mere depicting, inclusion and/or any use of the trademarks, design patents, commercial designations, titles and/or any other intellectual property in the content and/or in connection with the SERVICE. Depending on the right holder, the express prior written consent of CONTINENTAL, the Affiliate and/or a third-party right holder is required for using the trademarks, design patents, commercial designations, titles and/or any other intellectual property for any other purposes than those stated in this AUP, unless permissible under the applicable law.

The User shall not to assert any rights in the SERVICE or any intellectual property, in particular, but not limited to trademarks, design patents, commercial designations, titles, used by CONTINENTAL and/or the Affiliates in the content and/or in connection with the SERVICE.

e. The User shall not use automated methods (in particular data mining) to access data from the SERVICE, upload viruses, malware or malicious code or in any other way interfere with the proper functioning, integrity, operation or appearance of the SERVICE and the systems used for it.

f. The User shall not use the SERVICE in a manner that

- may cause damage to other users or impairs the use or the safety of the SERVICE;
- is not permitted under this AUP or under the AGREEMENT;
- violates the applicable law.

THE USER IS INFORMED THAT THEY SHALL VERIFY THAT ALL CONTENT GENERATED OR SHARED VIA THE SERVICE IS NOT ENCUMBERED WITH (UNLICENSED) COPYRIGHTS, INDUSTRIAL PROPERTY RIGHTS, NEIGHBORING RIGHTS OR OTHER THIRD-PARTY RIGHTS. THE USER WARRANTS AND ENSURES THAT ALL NECESSARY APPROVALS FOR THE CREATION AND USE OF THE CONTENT PURSUANT TO THIS AUP HAVE BEEN PROVIDED. IF PERSONS ARE DEPICTED OR AUDIBLE ON THE CONTENT, THE ADDITIONAL PRIOR WRITTEN CONSENT OF THOSE PERSONS MAY BE REQUIRED FOR THE PRODUCTION OF THE CONTENT. IN THIS EVENT, THE USER SHALL OBTAIN THE RELEVANT CONSENT FROM SAID PERSONS. IF THE USER INVOLVES THIRD PARTIES IN THE PRODUCTION OF THE CONTENT, THE USER SHALL MAKE SURE THAT IT IS GRANTED THE RIGHTS REQUIRED TO GRANT THE RIGHTS PURSUANT THIS SECTION.

THE USER IS INFORMED THAT MISLEADING, ADVERTISING, UNTRUE, DISCRIMINATORY, OFFENSIVE OR CRIMINALLY RELEVANT CONTENT IS PROHIBITED. IT IS ALSO PROHIBITED TO USE ANY TRADEMARKS, DESIGN PATENTS, COMMERCIAL DESIGNATIONS, TITLES AND/OR ANY OTHER INTELLECTUAL PROPERTY IN ANY CONTENT IN A WAY THAT DAMAGES OR HARMS THE REPUTATION AND/OR GOODWILL ASSOCIATED WITH CONTINENTAL AND/OR ITS AFFILIATES OR IN ANY OTHER WAY THAT NEGATIVELY IMPACTS OR MAY NEGATIVELY IMPACT SUCH REPUTATION AND/OR GOODWILL. CONTINENTAL RESERVES THE RIGHT TO DELETE OR HAVE DELETED ANY SUCH CONTENT AS WELL AS ANY CONTENT SUBMITTED ANONYMOUSLY OR UNDER A FALSE NAME AND TO EXCLUDE USERS FROM USING THE SERVICE.

2. Personal data protection

Privacy policy information can be viewed within the SERVICE or here [https://8675.ccp.continental.exchange]. CONTINENTAL reserves the right to change, adapt, delete parts of or add new parts to this data protection information at its own discretion, but within the scope of applicable legal regulations.

3. Information and credentials

- **a.** The User shall provide CONTINENTAL with true, accurate and complete information. By activating an account, the User may be requested to agree to the use of electronic means to receive communications.
- **b.** The User must keep its account credentials secret and may not disclose them to third parties - not even within its employer's company, unless otherwise agreed between its employer and CONTINENTAL. CONTINENTAL recommends the User to keep their username and password separately.
- **c.** If the User becomes aware that an unauthorized third party has obtained knowledge of the access data, or if there is at least a suspicion that this is the case, the User must immediately create or apply for a new password.
- **d.** CONTINENTAL is entitled to block access if there is reasonable suspicion of misuse of access by third parties.
- **e.** CONTINENTAL is not responsible for any loss or damage resulting from failure to comply with these requirements.

4. Third party links and contents.

- **a.** Unless otherwise agreed in the AGREEMENT, in the event that the SERVICE contains links to third-party online contents, CONTINENTAL is not responsible for it and such online contents are not regularly verified, monitored or controlled for accuracy or completeness on the part of CONTINENTAL.
- **b.** If the User accesses these third-party websites, the User does so at his own risk and becomes subject to the terms of use and the privacy policies of such third-party online content.
- **c.** The User shall inform CONTINENTAL in the event that a link to a third-party content is found to prevent the SERVICE from functioning correctly or to violate applicable law.

5. Export Control

The User is informed that items related to the SERVICE (e.g. software) can be subject to Export Control regulations; therefore the User shall comply with all applicable Export Control regulations and laws. In case of doubts, the User shall ask clarifications to its employer.

6. Continental's rights and remedies

- **a.** If the User becomes aware of any content or activity that violates this AUP, the User shall take all reasonable steps to notify CONTINENTAL immediately and to prevent such content from being transmitted to or stored on the CONTINENTAL network.
- **b.** If the User fails to comply with this AUP, CONTINENTAL may take actions ranging from warnings to disablement, suspension or termination of the SERVICE.

7. Changes to this Acceptable Use Policy

CONTINENTAL reserves the right to update this AUP from time-to-time, in its sole discretion, effective upon posting a revised copy of the updated AUP within the SERVICE. Any use of the SERVICE after such modification shall constitute acceptance of such modification.

Status 06.2024

SERVICE SPECIFIC TERMS FOR CAEDGE

SERVICE SPECIFIC TERMS FOR CUSTOMER DEVELOPMENTS

10. GENERAL

10.1 These SERVICE SPECIFIC TERMS FOR CUSTOMER DEVELOPMENTS ("**DEVELOPMENT TERMS**") govern the provision of the CAEdge functionalities for creation of CUSTOMER CONTENT via the SERVICE.

10.2 The DEVELOPMENT TERMS supplement the GENERAL T&Cs. In case of conflicts, the DEVELOPMENT TERMS shall prevail.

11. CUSTOMER DEVELOPMENTS

11.1 CUSTOMER and CUSTOMERs users may create, develop, integrate, import, store, export, transmit, display, distribute or use software artefacts and other content in or through use of the SERVICE ("**CUSTOMER CONTENT**") as set forth in the SERVICE DESCRIPTION. This may include also user related data from internal as well as external parties that contribute to CUSTOMER CONTENT.

11.2 CUSTOMER may create CUSTOMER CONTENT solely by its own users or jointly in cooperation with users of other CONTINENTAL customers of the SERVICE ("**PROJECT PARTNERS**"). CUSTOMER is solely responsible for the management of CUSTOMER CONTENT via the SERVICE and for the management of the cooperation with CUSTOMER's PROJECT PARTNERS, including but not limited to the assignment of access rights to users of CUSTOMER and CUSTOMER's PROJECT PARTNERS, if any, and the uploading and disclosing of trade secrets and other sensitive information via the SERVICE.

11.3 CONTINENTAL may make available via the SERVICE certain THIRD-PARTY SERVICES, in particular development tools or of-the-shelf software artefacts ready for integration into or combination with CUSTOMER CONTENT. CONTINENTAL does not endorse these THIRD-PARTY SERVICES or act as licensor or provider thereof. CUSTOMER acknowledges that THIRD-PARTY SERVICES may be subject to the acceptance of certain terms and conditions of their respective providers or licensors. CUSTOMER's use of such THIRD-PARTY SERVICES is on CUSTOMER's own risk and account. **Section 12.8** of the GENERAL T&Cs applies accordingly.

11.4 CUSTOMER agrees to abide by (and be responsible for its users compliance with) applicable laws and regulations regarding its access, generation, use and distribution of CUSTOMER CONTENT.

11.5 CONTINENTAL accepts no responsibility or liability of any nature with respect to CUSTOMER CONTENT. CUSTOMER and CUSTOMER's PROJECT PARTNERS (if any) are solely responsible for the accuracy, quality, integrity, and legality of CUSTOMER CONTENT and the way CUSTOMER CONTENT is generated, used, shared and distributed via the SERVICE.

11.6 CUSTOMER warrants, that use of the SERVICE complies with the applicable antitrust laws. This applies – in particular - to the extent, that CUSTOMER and CUSTOMER´s PROJECT PARTNERS and / or their affiliated companies are actual or potential competitors on the market relevant for their cooperation via the SERVICE. CUSTOMER is responsible to implement all precautions and / or safeguards which are necessary to ensure compliance with the applicable antitrust laws. CONTINENTAL does not accept any liability with regard to infringements of such laws by CUSTOMER, CUSTOMER's PROJECT PARTNERs or their respective users.

12. RIGHTS IN CUSTOMER CONTENT

12.1 CUSTOMER represents and warrants that CUSTOMER owns all necessary rights to any CUSTOMER CONTENT CUSTOMER discloses, uploads to or shares via the SERVICE and that CUSTOMER has the necessary authority to transmit and disclose CUSTOMER CONTENT using the SERVICE.

12.2 CONTINENTAL has no rights, title or interest in any CUSTOMER CONTENT, except for the rights explicitly granted to CONTINENTAL under this AGREEMENT. CUSTOMER retains all rights, title, and interest in and to CUSTOMER CONTENT that have arisen in CUSTOMER's position or have been transferred to CUSTOMER by operation of law or legal transaction. The allocation of rights in CUSTOMER CONTENT generated jointly by CUSTOMER's users and users of CUSTOMER's PROJECT PARTNERS is subject to the individual agreements between CUSTOMER and CUSTOMER's PROJECT PARTNERS.

12.3 By using the SERVICE, uploading or sharing CUSTOMER CONTENT, CUSTOMER hereby grants to CONTINENTAL a non-exclusive worldwide license to use, copy, store, process, transmit, retrieve, and display such CUSTOMER CONTENT in connection with the provision of the SERVICE for CUSTOMER and CUSTOMER's PROJECT PARTNERS (if any).

12.4 CUSTOMER will defend, indemnify and hold CONTINENTAL harmless from and against any claim brought against CONTINENTAL or its affiliates by a third party, any final award of damages or settlement amount, and any liabilities or expenses incurred by CONTINENTAL or CONTINENTAL's affiliates (including reasonable attorneys' fees) as a result of any claim arising out of or relating to CUSTOMER CONTENT, including (but not limited to) any claim that the CUSTOMER CONTENT violates any applicable law, regulation, or the intellectual proprietary rights of others. CUSTOMER cannot invoke the fact that CUSTOMER CONTENT was jointly generated by CUSTOMER and CUSTOMER's PROJECT PARTNERS.

13. CONFIDENTIALITY & SECRECY OF CUSTOMER CONTENT

13.1 CUSTOMER understands and acknowledges CUSTOMER CONTENT uploaded and shared via the SERVICE is disclosed to any given PROJECT PARTNERS of the CUSTOMER and their respective users, if respective access rights have been granted by CUSTOMER. CONTINENTAL is not responsible for the confidential treatment of CUSTOMER CONTENT or any other CUSTOMER information by CUSTOMER's PROJECT PARTNERS and their respective users.

13.2 CUSTOMER agrees to not disclose, upload or share to the SERVICE any CUSTOMER CONTENT that is or contains information that has the potential for damage that threatens a company's existence, or is of long-term nature, or is not limited to a single company, as defined by VDA ISA 6.0 (https://www.vda.de/en/topics/digitization/data/information-security) classification "very high" ("**STRICTLY CONFIDENTIAL INFORMATION**"). CUSTOMER shall provide a classification for all transferred CUSTOMER CONTENT in a written form before the CUSTOMER CONTENT is transferred to the SERVICE.

13.3 CONTINENTAL is not permitted to disclose this AGREEMENT or access and disclose any CUSTOMER CONTENT except as necessary to maintain or provide the SERVICE without CUSTOMER's prior consent, unless required to do so pursuant to applicable law or regulation or requests or orders of judicial, governmental or regulatory entities (including without limitation subpoenas).

13.4 CONTINENTAL and its service providers implement and maintain state of art technical and organizational measures as set out in the SERVICE DESCRIPTION to prevent any unauthorized access to CUSTOMER CONTENT. The transfer of CUSTOMER CONTENT to the SERVICE is secured with a secure protocol (https) and stored in a private cloud on encrypted partitions.

13.5 CUSTOMER remains responsible for (i) properly assigning the access rights for its users and users of CUSTOMER's PROJECT PARTNERS, (ii) its users (as well the users of CUSTOMER's PROJECT PARTNERS) access to and use of CUSTOMER CONTENT, (iii) the adequate backup and protection of its CUSTOMER CONTENT, and (iv) the secure transmission of CUSTOMER CONTENT to the SERVICE.

SERVICE SPECIFIC TERMS FOR VECU CREATOR

10. GENERAL

10.1 These SERVICE SPECIFIC TERMS FOR VECU CREATOR ("**VECU TERMS**") govern the provision of the CAEdge functionalities for creation of virtually simulated electronic control units and electronic control unit partitions ("**VECU**") and the deployment of CUSTOMERs software architecture on VECU for testing and validation purposes via the SERVICE.

10.2 The VECU TERMS supplement the GENERAL T&Cs. In case of conflicts, the VECU TERMS shall prevail.

11. VECU CREATOR

11.1 CUSTOMER can use VECU CREATOR for creating and operating VECUs in a dedicated cloud instance. CUSTOMER can select the operating systems of interest (with Classic AutoSAR, Android, Linux, QNX OS + AUTOSAR Adaptive) to be installed on the VECU as made available in the SERVICE. CUSTOMER can deploy and execute CUSTOMER's own application software ("**CUSTOMER SW**") on VECU for testing and validation of CUSTOMER SW.

11.2 CUSTOMER SW can either be created by using the SDKs provided within the SERVICE (see SERVICE SPECIFIC TERMS FOR CUSTOMER DEVELOPMENTS) or upload externally created CUSTOMER SW into the repository provided within the SERVICE.

11.3 VECU CREATOR is intended for testing of basic functionality of CUSTOMER SW on the created VECU, including module tests, integration tests, and system tests. In addition, ECU communication, network connectivity and calling of external cloud services/resources, complementing traditional system tests. Load-testing, Security test and other stress-tests are not feasible. VECU CREATOR shall support CUSTOMER in identifying existing errors, defects, and bugs in CUSTOMER SW, but cannot verify the absence of such.

11.4 CUSTOMER represents and warrants that CUSTOMER owns all necessary rights to any CUSTOMER SW CUSTOMER discloses, uploads to or shares via the SERVICE and that CUSTOMER has the necessary authority to transmit and disclose CUSTOMER SW using the SERVICE.

11.5 CUSTOMER will defend, indemnify and hold CONTINENTAL harmless from and against any claim brought against CONTINENTAL or its affiliates by a third party, any final award of damages or settlement amount, and any liabilities or expenses incurred by CONTINENTAL or CONTIENTAL's affiliates (including reasonable attorneys' fees) as a result of any claim arising out of or relating to CUSTOMER SW, including (but not limited to) any claim that the CUSTOMER SW violates any applicable law, regulation, or the intellectual proprietary rights of others.

11.6 For the avoidance of doubt, CUSTOMER SW shall be considered as CUSTOMER CONTENT and the provisions of the AGREEMENT concerning CUSTOMER CONTENT shall apply.

12. WARRANTY

12.1 CONTINENTAL accepts no responsibility or liability of any nature with respect to CUSTOMER SW. CUSTOMER is solely responsible for the accuracy, quality, integrity, and legality of CUSTOMER SW. CUSTOMER remains solely responsible for determining the readiness of the CUSTOMER SW for real world application according to the applicable standards and regulations for software development.

12.2 CONTINENTAL provides the functionalities for testing and validating of CUSTOMER SW as service with no obligation to provide a certain result. CONTINENTAL shall only be obliged to ensure the proper execution of testing and validation processes triggered and controlled by CUSTOMER in accordance with the parameters defined by CUSTOMER. CONTINENTAL accepts no responsibility or liability of any nature with respect to the accuracy or reliability of the results of testing and validation of CUSTOMER SW via the SERVICE. The provisions of the German Civil Code on contracts for work ("*Werkvertragsrecht*") shall not apply.

13. CONFIDENTIALITY & SECRECY OF CUSTOMER SW

13.1 CUSTOMER agrees to not disclose, upload or share to the SERVICE any CUSTOMER SW that is or contains information that has the potential for damage that threatens a company's existence, or is of long-term nature, or is not limited to a single company, as defined by VDA ISA 6.0 (https://www.vda.de/en/topics/digitization/data/information-security) classification "very high" ("**STRICTLY CONFIDENTIAL INFORMATION**"). CUSTOMER shall provide a classification for all transferred CUSTOMER SW in a written form before the CUSTOMER SW is transferred to the SERVICE.

13.2 CONTINENTAL is not permitted to disclose this AGREEMENT or access and disclose any CUSTOMER SW except as necessary to maintain or provide the SERVICE without CUSTOMER's prior consent, unless required to do so pursuant to applicable law or regulation or requests or orders of judicial, governmental or regulatory entities (including without limitation subpoenas).

13.3 CONTINENTAL and its service providers implement and maintain state of art technical and organizational measures as set out in the SERVICE DESCRIPTION to prevent any unauthorized access to CUSTOMER SW. The transfer of CUSTOMER SW to the SERVICE is secured with a secure protocol (https) and stored in a private cloud on encrypted partitions.

13.4 CUSTOMER remains responsible for (i) properly assigning the access rights for its users, (ii) its users access to and use of CUSTOMER SW, (iii) the adequate backup and protection of CUSTOMER SW, and (iv) the secure transmission of CUSTOMER SW to the SERVICE.

SERVICE DESCRIPTION FOR CAEDGE

10. CAEDGE

10.1 CAEdge is a comprehensive framework for the development of automotive software leveraging cloud and on-premise resources. The framework is modular, scalable, and extendable.

10.2 The full scope of CAEDGE is

10.2.1 Collaborative software development

10.2.2 Decoupling of SW development from hardware

10.2.3 Virtualization and simulation of Automotive OSs

10.2.4 Validation and improvement of system functions

10.3 The currently available components are:

10.3.1 Basic functionality with user management

10.3.2 VECU Creator

11. BASIC FUNCTIONALITY

11.1 The basic functionality package of CAEdge is comprised of cloud-based workbenches for development and execution of SDV Software Packages (Automated DevOps workflows as well as interactive development / debugging / testing).

11.2 PC based tooling to simplify the onboarding and access of the SDV developers to the CAEdge provided workbenches, that include:

11.2.1 Connect generic IDEs with CAEdge vECU instances,

11.2.2 Scripts to access cloud resources seamlessly,

11.2.3 Possibility aggregate and view DLT logs

11.2.4 Tools to visualize the screen content of systems running in the cloud or in connected on-premise environments,

11.2.5 Debugging tools to assess the status of the cloud and on-premise hosted execution environments.

11.2.6 CAEdge managed assets include SW assets such as standard automotive operating systems and Middleware (AUTOSAR, Android, Linux) components and Internet-of-Things connector components deployed to the development boards and simulated devices.

SERVICE DESCRIPTION FOR CAEDGE

CAEdge vECU Creator - Service Description & Service Level Agreement (SLA)

Name of Service

CAEdge - Continental Automotive Edge
vECU Creator – virtual ECU Creator

Introduction & Short Description

This documentation shall serve as general description of Continental's service offerings related to CAEdge – vECU Creator (in the following also referred to as the "Service"). Please note that the Service exclusively comprises those services, deliverables, features and functionalities that are expressly documented as part of the Service within this documentation. Services or deliverables not explicitly declared as covered by the Service will not be provided.
CAEdge vECU Creator provides a secure/robust supporting software development execution environment in the context of the Software Defined Vehicle (SDV). It can host one or more Automotive OSs (Classic AutoSAR, Linux, Android & QNX) and establish standard communication (Ethernet, CAN) between them as configured by the user. It provides functional parity to physical ECU for application development and testing. It also enables ECU level testing environment.

1. SERVICE DESCRIPTION

CAEdge is a cloud-based **framework** which is designed for projects where:

- **SW** development is **decoupled from HW development.**
- **virtualization** and **simulation** is used to parallelize and speed up development time.
- **seamless collaboration** and delivery of software with customers and suppliers within the SW lifecycle chain is needed.
- **vehicle data** is used to validate and improve system functions.

1.1 The CAEdge Framework Elements

vECUCreator_Included = Part of the vECU Creator service

AdditionalLicenseRequired = Can be added to the vECU Creator service using a different subscription model

- **Cloud-based workbenches** (see below) for development and execution of SDV Software Packages (Automated DevOps workflows as well as interactive development / debugging / testing) **AdditionalLicenseRequired**
- **PC based tooling** to simplify the onboarding and access of the SDV developers to the CAEdge provided workbenches, that include:
  - **IDEs** with CAEdge specific configurations, **AdditionalLicenseRequired**
  - **Scripts to access** cloud resources seamlessly, **vECUCreator_Included**
  - Tools to **visualize the screen** content of systems running in the cloud or in connected on-premise environments, **vECUCreator_Included**
  - **Debugging tools** to assess the status of the cloud and on-premise hosted execution environments. Full Feature set: **AdditionalLicenseRequired**
- **CAEdge managed assets** include
  - **Development boards** (HDKs), **AdditionalLicenseRequired**
  - a **HW Farm**, **AdditionalLicenseRequired**
  - **SW assets** such as standard automotive operating systems and Middleware (AUTOSAR, Android, Linux) components, **AdditionalLicenseRequired**
  - and **Internet-of-Things connector** components deployed to the development boards and simulated devices. **vECUCreator_Included**

1.1.1 CAEdge Workbenches Overview

- *Engineering Workbench* is used to develop and validate SW in the Cloud. **AdditionalLicenseRequired**
- *HDK Workbench* is used to deploy application in real hardware or virtual ECU. **vECUCreator_Included**

- *vECU Creator Workbench* is used to create virtual ECU that is supported by *Engineering Workbench* and *HDK Workbench.* **vECUCreator_Included**
- *Service Development Workbench* is used to develop additional *CAEdge Services.* **AdditionalLicenseRequired**

2. SERVICE **DESCRIPTION**

CAEdge vECU Creator is a cloud-based **framework** which is designed for projects where:

- **SW** development is **decoupled from HW development.**
- **Virtualization** and **simulation** are used to parallelize and speed up development time.
- **Deployment** of application to POSIX system
- **Seamless collaboration** and delivery of software with customers and suppliers within the SW lifecycle chain is needed.
- **Vehicle data** is used to validate and improve system functions.

CAEdge vECU Creator consists of

- **Cloud-based workbenches** (see below) for development and execution of SDV Software Packages (Automated DevOps workflows as well as interactive development / debugging / testing)
- **PC based tooling** to simplify the onboarding and access of the SDV developers to the CAEdge provided workbenches, that include:
    - **Integration with standard IDEs** and CAEdge
    - **Scripts to access** cloud resources seamlessly,
    - Tools to **visualize the screen** content of systems running in the cloud or in connected on-premise environments,
    - **Debugging tools** to assess the status of the cloud and on-premise hosted execution environments.
- **CAEdge managed assets** include
    - **Development boards** (HDKs)In a **HW Farm**,
    - **SW assets** such as standard automotive operating systems and Middleware (AUTOSAR, Android, Linux) components,
    - and **Internet-of-Things connector** components deployed to the development boards and simulated devices.

3. CAEDGE WORKBENCHES OVERVIEW

- *Engineering Workbench* is used to develop and validate SW in the Cloud.
- *HDK Workbench* is used to deploy application in real hardware (when available and connected) or virtual ECU.
- *vECU Creator Workbench* is used to create virtual ECU that is supported by *Engineering Workbench* and *HDK Workbench.*
- *Service Development Workbench* is used to develop additional *CAEdge Services.*

4. SUPPORT LANGUAGE

English

5. SERVICE LANGUAGE

English

6. PROCESSUAL **AGREEMENTS**

For proper usage of the Service by the Customer, both the Provider and the Customer have assigned responsibilities in the meaning of deliverables they have to provide. The possible Obligations Levels are:

- **Standard** = respective activity/product have to be delivered by the respective party as mandatory part of the Service.

- **Optional** = respective activity/product could be delivered but have to be analyzed and further agreed, case by case, as particular situations.
- **NOT provided** = activity/product is not delivered by this service, although some other IT services might deliver such activities/products.

Deliverables

7. PROVIDER **DELIVERABLES**

Fulfillment of defined Service Requests

- Specific structure configuration for the target CAEdge services (e.g.: Tenant/Project Structure - create, update, etc.) **Standard**
- Project specific access management to CAEdge Services applying defined Role Model **Standard**
- Creation of 'new tenants/project' **Optional**
- Decommissioning tenants/projects no longer needed **Optional**
- Creation of service objects (e.g.: HDK service) **Standard**
- Access to the service objects **Standard**
- Assigning roles and rights to users **Standard**

Implementation of defined Standard Changes (pre-authorized changes with low implementation risk following a defined work instruction)

- Describe the defined Standard Changes and the proper way to request them (Standard Changes are equivalent with Standard Request) **Standard**

Support and Incidents Resolution (via tickets)

- Service functionality Issues for supported services **Standard**
- Access permissions Issues for supported services **Standard**
- Service malfunction – collect and clarify with provider **Standard**
- Answer questions and requests for information **Standard**
- Platform availability and connectivity **Standard**
- Ensure performance and resources for the platform **Standard**

Training (for end-users)

- Organize Training Sessions for end-users **Optional**
- User manual is available **Standard**

Implementation of small enhancements via Change Requests

- Analysis and implementation of small enhancements (Standard Changes are equivalent with Standard Request) **Standard**
- Communication of Bugs and Change Requests to Dev team **Standard**
- Contribute to Change prioritization of BUG's and requests **Standard**

Upgrades to new releases for the supported applications

- Upgrades to new releases for the supported services **Standard**
- Version upgrades of the platform will take place according to the CAEdge Release cadence **Standard**
- Installation and major version upgrades of the contained services **Standard**

Related Infrastructure Management for proper provisioning of the service

- Coordinate resolution of Infrastructure related issues that impact proper functioning of the delivered service **Standard**
- Management of code for infrastructure and service components **Standard**

Vendor and Contract Management

- Continental may connect the Customer with the Software Stack vendors for license procurement. This includes:
    - Contract offer with Vendor **Optional**
- Management of Continental support resources **Optional**
- Management of Continental development resources **Optional**

License Management for 3rd Party Software Stacks

- License monitoring and usage optimization **Standard**
- Software Licensing used in services **Standard**
- Automated service monitoring and reporting of the availability **Standard**

Implementation of small enhancements via Change Requests

- Adjusting the layout 'look and feel' for individual projects **Optional**
- Customer specific services, tools and workflows **Optional**
- Integration support to customer specific test framework **Optional**
- Customer specific configuration and synchronization jobs with customer databases. **Optional**

8. CUSTOMER DELIVERABLES

For the Provider to properly deliver the described service, the Customer have to provide the following deliverables in the agreed time and quality.

- Providing a detailed request by using the integrated Service Desk in the Continental Cooperation Portal. (Use CCP Support button.)
- Ticket via CCP Jira Service Desk (Use CCP Support button.)
- Provide precise information that is needed to solve the issue (i.e. logs, screenshots, description of the issue)
- Information about the customer (i.e. user ID / username, email address, mobile number, role)
- Identify the impacted service (i.e. HDK Service, vECU Service etc.)
- Provide information about user changes (left company / changed role)
- Signed AGB
- Project coordinator from each company
- Projected number of users over time (forecast)
- Provide precise information for non-standard functionality required
- Provide support contact and process description for non-standard functionality
- Provide Licenses for project specific content, such as virtualization environments and toolchains for software building, testing and deployment.
    - **For the Software Stacks running inside VECU Creator Execution Environment Conti is not reselling the licenses of such stacks. The customer has to make sure valid licenses are available.**

9. OUT OF SCOPE

All objects, processes, tasks not selected in the "Provider Deliverables" section are considered by default "Out of Scope".
Additional Out-of-Scope:

Fulfillment of defined Service Requests

- Diagnostics and problem solving on non-Continental networks **NOT Provided**
- Any changes to customer provided data (needs to be done by customer) **NOT Provided**
- Diagnostics and problem solving on non-Continental provided vECU partitions **NOT Provided**

Support and Incidents Resolution (via tickets)

- Support for Applications installation Issues where pre-requisites are not met (Operating Systems, Network connectivity) **NOT Provided**
- Customer infrastructure upgrades to meet prerequisites for correct platform functionality **NOT Provided**

Upgrades to new releases for the supported applications

- Integration of legacy tools **NOT Provided**

Service support information

10. FIRST LEVEL SUPPORT DONE BY SERVICE DESK

First Line Resolution

11. INCIDENT MANAGEMENT

CAEdge Service via CCP Service Desk Portal.

12. CUSTOMER FEEDBACK

CAEdge Framework and vECU Creator appreciates customer feedback including recommendations for feature enhancements.

13. INCIDENT MANAGEMENT

The CAEdge users can interact with the Continental Cooperation Portal (CCP) Service Desk Team during the *Attended Operation hours* as shown in the Service Quality table below.
CCP Service Desk Hotline: +49 511 36734253
CCP_Support@continental.com

14. KNOWLEDGE MANAGEMENT

CAEdge User Manual is offered to the end customer via the CAEdge Framework front end.

15. PROBLEM MANAGEMENT

All CAEdge users have access to the CCP Service Desk Jira System. The Service Desk contains issue types for:

- general access topics,
- CCP Application problems and requests,

and specially for CAEdge:

- CAEdge project/tenant creation & maintenance issues,
- Specific problems and improvement requests for the CAEdge services.

The CAEdge related issue types are migrated to CAEdge internal solution tickets and then:

- analyzed by the CAEdge support team,
- assigned to the corresponding Team for resolution,
- leading to a fix in the CAEdge Framework.

The Requestor will be informed about the progress in the Service Desk Request ticket.

Communication

- CAEdge stakeholders will be asked by the responsible Customer Project Manager for their input prior to CAEdge PI-Plannings.
- The CCP Landing Page will show information banner about planned downtimes.
- CCP Service desk will inform all users about emergencies and downtimes via Information Banners in the system and email notifications.

Service Quality

CAEdge Platform Availability Hours **24 x 7** (An agreed time period (Operation time) when a particular IT service should be available. Synonym for agreed service time)
Attended Operation hours of the CCP Service Desk **Mo – Fr: 8:00 – 18:00 CET** (The operation hours of an IT service in which the service personnel is attending the service provision, except bank holidays on provider's site. (betreuter Betrieb)) Extra availability can be added on request. (24 x 5, 24 x 7)
Availability excl. planned maintenance activities. **99,2%** (The ratio not the total time an IT service is capable of being used during one month)
Maintenance Window **8h, every (1st, 2nd, 3rd) Saturday in a month and on demand (in case of priority issue)** (Will be upon and coordinated with the projects.)
Incidents in Backlog **Monthly Report by CCP Service Desk on Incident Ticket Status** (The intention is to monitor and show historical indicators showing what Incident amount was left open in the past with a weekly resolution.)
Max. time to Restore Service **24h** (The maximum time taken to Restore an IT Service after a Failure (from down to complete up (Normalbetrieb)). MTRS is measured from when the IT Service fails until it is fully restored and is fully restored and delivering its normal functionality (recovery time + emergency operation time))
Change Requests in Backlog Monthly Report by CCP Service Desk on Incident Ticket Status is provided (# of changes with planned end date < closed date (bzw. current date))
Changes in Time **CAEdge provides continuously a Project Status Report showing the Status of the planned changes** (Percentage of Changes, where planned dates and actual dates are equal)

Service Exceptions

The Service Commitment does not apply to any unavailability, suspension, termination, and performance issues:

1. caused by factors outside of the providers reasonable control including any force majeure event or Internet access or related problems beyond.
2. that result from any voluntary actions or inactions by the customer (e.g., scaling of provisioned capacity, misconfiguring security groups, VPC configurations or credential settings, disabling encryption keys or making encryption keys inaccessible, etc.).
3. that result from customers equipment, software, or other technology,
4. that result from customers not following this SLA and or Continental Terms and conditions.

DATA PROCESSING AGREEMENT (DPA) FOR CAEDGE

STANDARD CONTRACTUAL CLAUSES on Data Processing acc. to Art. 28 EU GDPR

related to the AGREEMENT

between

CAEdge Customer

- hereinafter referred to as "**Controller"** -

and

Continental Automotive Technologies GmbH

Continental Plaza 1
30175 Hannover

- Processor hereinafter referred to as "**Processor"** -

- jointly referred to as **"Parties"** -

These Standard Contractual Clauses ((EU) 2021/915)) stipulate the legal obligations of the Parties regarding data protection resulting from the processing of personal data related to the AGREEMENT
(hereinafter also referred to as "**contract**").

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description *of processing(s)*

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the

security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION**: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 (thirty) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub- processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub- processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in

order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub- processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to* the *controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'daa protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay

if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification *of personal data breach*

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with *the Clauses and termination*

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored

within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s):

CAEdge Customer as identified in the AGREEMENT

Processor(s):

Continental Automotive Technologies GmbH
Continental Plaza 1
30175 Hanover

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

☐ Clients ☐ Visitors
☐ Event participants ☐ Service users
☐ Communication participants ☐ Subscribers
☐ Interested parties
☐ Supplier and/ or Service Provider (individual contacts at these vendors)
☐ Employees ☐ Applicants
☐ Former employees ☐ Apprentices/ interns
☐ Employees relatives ☐ Consultants
☐ Sales representatives ☐ Shareholders / bodies
☐ Contact persons for business ☐ Suppliers and service providers
☐ Business partners
☒ Other (please specify): ___Data provided by user (user generated content)

Categories of personal data processed

……..

General data/ private contact details

☐ Names Personal profiles ☐ Image
☐ Private address data ☐ Date of birth
☐ ID card data (e.g. Passport, Social Security, Driving License)
☒ Other (please specify): Data provided by user (user generated content)

Contract data

☐ Settlement and payment data ☐ Bank details/ credit card data
☐ Financial Standing/ Creditworthiness ☐ Contract histories
☐ Other (please specify): _____

Professional data

☐ Personal Details ☐ Position and Employment Details
☐ Performance Management ☐ Qualification and Education Details
☐ Salary or Social Security Data ☐ Absence from Work
☐ Other please specify: _____

Service and IT usage data

☐ Device identifiers ☐ Usage and connection data
☐ Image / video data ☐ Telecommunication data/ message content
☐ Audio / voice data ☐ Identification data
☐ Access data ☐ Authorization
☐ Meta data
☒ Other (please specify): __ Data provided by user (user generated content)

Sensitive data processed (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.

Special categories of personal data

☐ Race or Ethnic Origin
☐ Religious or Philosophical Beliefs
☐ Physical or Mental Health
☐ Political Opinions
☐ Biometric Data
☐ Genetic Data
☐ Trade Union Membership
☐ Sexual Life
☐ Criminal Offences, Convictions or Judgments

Nature of the processing

…Storage of data

Purpose(s) for which the personal data is processed on behalf of the controller

Fulfill usage contract

Duration of the processing

During the contract/usage

……

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

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

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

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

1. Physical Access Control

Safeguarding admission/access to processing systems with which processing is carried out against unauthorized parties (e.g. through physical property protection: fence, gatekeeper, personnel barrier, turnstile, door with card reader, camera surveillance, organizational property security, regulation on access authorizations, access registration)

The following technical and organizational measures have been implemented by the Processor for the processing of personal data described in these Clauses:

☒	Alarm system
☒	Automatic access control system
☐	Locking system with code lock
☐	Biometric access barriers
☐	Light barriers/motion sensors
☐	Manual locking system including key regulation (key book, key issue)
☒	Visitor logging
☒	Careful selection of security staff
☒	Chip cards/transponder locking systems
☒	Video monitoring of access doors
☒	Safety locks
☒	Personnel screening by gatekeeper/reception
☒	Careful selection of cleaning staff
☒	Obligation to wear employee/guest ID cards
☐	Other:

2. Data Access Control/User Control

Prevention of third parties using automatic processing systems with equipment for data transmission (authentication with user and password).

The following technical and organizational measures have been implemented by the Processor for the, processing of personal data described in these Clauses:

☒	Authentication with user name/password (passwords assigned based on the valid password regulations)
☒	Usage of intrusion detection systems
☒	Usage of anti-virus software
☒	Usage of a software firewall
☒	Creation of user profiles
☒	Assignment of user profiles to IT systems
☒	Usage of VPN technology
☒	Encryption of mobile data storage media
☒	Encryption of data storage media in laptops
☒	Usage of central smartphone administration software (e.g. for the external erasure of data)
☐	Other:

3. Data Usage Control/Data Storage Media Control/Memory Control

Prevention of unauthorized reading, copying, changing or erasure of data storage media (data storage media control), prevention of unauthorized entry of personal data and unauthorized access to it, changing and deleting saved personal data (memory control). Ensuring that the parties authorized to use an automated processing system only have access to the personal data appropriate for their access authorization (e.g. through authorization concepts, passwords, regulations for leaving the company and for moving employees to other departments.) (data usage control).

The following technical and organizational measures have been implemented by the Processor for the, processing of personal data described in these Clauses:

☒	Roles and authorizations based on a *"need to know principle"*
☒	Number of administrators reduced to only the "essentials"
☒	Logging of access to applications, in particular the entry, change and erasure of data
☒	Physical erasure of data storage media before reuse
☒	Use of shredders or service providers
☒	Administration of rights by defined system administrators
☒	Password guidelines, incl. password length and changing passwords
☒	Secure storage of data storage media
☒	Proper destruction of data storage media (DIN 66399)
☒	Logging of destruction
☐	Other:

4. Transfer Control/Transportation Control

Ensuring that the confidentiality and integrity of data is protected during the transfer of personal data and the transportation of data storage media (e.g. through powerful encryption of data transmissions, closed envelopes used in mailings, encrypted saving on data storage media).

The following technical and organizational measures have been implemented by the Processor for the processing of personal data described in these Clauses:

☒	Establishment of dedicated lines or VPN tunnels
☒	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☒	E-mail encryption
☒	Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines
☒	In case of physical transportation: careful selection of transportation personnel and vehicles
☒	Transmission of data in an anonymized or pseudonymized form
☒	In case of physical transportation: secure containers/packaging
☐	Other:

5. Entry Control/Transmission Control

Ensuring that it is possible to subsequently review and establish which personal data has been entered or changed at what time and by whom in automated processing systems, for instance through logging (entry control).

Depending on the system, ensuring that it is possible to review and determine to which offices/locations personal data has been transmitted or provided using equipment for data transmission, or to which offices/locations it could be transmitted (transmission control).

The following technical and organizational measures have been implemented by the Processor for the, processing of personal data described in these Clauses:

☒	Logging of the entry, change and erasure of data
☒	Traceability of the entry, change and erasure of data through unique user names (not user groups)
☒	Assignment of rights for the entry, change and erasure of data based on an authorization concept
☒	Creating an overview showing which data can be entered, changed and deleted with which applications
☒	Maintaining forms from which data is taken over in automated processing
☐	Other:

6. Availability Control/Restoration/Reliability/Data Integrity

Ensuring that systems used can be restored in case of a disruption (restorability). Ensuring that all system functions are available and that any malfunctions are reported (reliability). Ensuring that saved personal data cannot be damaged through system malfunctions (data integrity). Ensuring that personal data is protected from accidental destruction or loss (availability control), e.g. by implementing appropriate back-up and disaster recovery concepts.

The following technical and organizational measures have been implemented by the Processor for the, processing of personal data described in these Clauses:

☒	Uninterruptible Power Supply (UPS)
☒	Devices for monitoring temperature and moisture in server rooms
☒	Fire and smoke detector systems
☒	Alarms for unauthorized access to server rooms
☒	Tests of data restorability
☒	Storing data back-ups in a separate and secure location
☒	In flood areas the server is located above the possible flood level
☒	Air conditioning units in server rooms
☒	Protected outlet strips in server rooms
☒	Fire extinguishers in server rooms
☒	Creating a back-up and recovery concept
☒	Creating an emergency plan
☐	Other:

7. Separation Control/Separability

Ensuring that data processed for different purposes can be processed separately (for instance through logical separation of customer data, specialized access controls (authorization concept), separating testing and production data).

The following technical and organizational measures have been implemented by the Processor for the, processing of personal data described in these Clauses:

☒	Physically separated storing on separate systems or data storage media
☒	Including purpose attributions/data fields in data sets
☒	Establishing database rights
☒	Logical client separation (software-based)
☒	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☒	Separation of production and testing systems
☐	Other:

ANNEX IV: LIST OF SUB-PROCESSORS

Sub-processor (Company Name, Address)	Service Type	Location of data center / processing	Protection measures (DPA, SCC, BCR, certificates etc)
Amazon Web Service	CloudService	Ireland	DPA