Hewlett Packard Enterprise

HPE Agreement Number(s) where required: ……
HPE entity: ……..
Customer: ……
Effective Date (if applicable): ……
Term Length (if applicable): ……..

HPE CUSTOMER TERMS - SOFTWARE-AS-A-SERVICE

1. **Scope and Parties.** These HPE Customer Terms for Software-as-a-Service (the "Agreement") govern the purchase, access and use of software-as-a-service from the Hewlett Packard Enterprise entity receiving the Order (defined below) ("HPE") by the Customer entity identified below ("Customer"). The terms of this Agreement become effective when HPE accepts Customer's order, upon renewal of an order or upon Customer's use of HPE SaaS (defined below) ("Effective Date"), and will remain in effect unless terminated pursuant to Section 19 (Termination).

2. **HPE Software-as-a-Service.** "HPE Software-as-a-Service" or "HPE SaaS" mean the HPE branded online software solutions that HPE makes available for Customer use through a network connection, each as described in the applicable supporting material and other exhibits or attachments that are each made a part of this Agreement (collectively, "Supporting Material"). The terms for use of each HPE SaaS is stated in the Supporting Material. Supporting Material may include service descriptions, data sheets, statements of work and their applicable exhibits, addenda, and attachments which may be available to Customer in hard copy or by accessing an HPE website. In the event of a conflict, Supporting Material takes precedence over this Agreement.

3. **Orders.** Customer may place orders for HPE SaaS through our website, customer-specific portal, or by letter, fax, or e-mail (each upon HPE's acceptance, an "Order"). The term of each HPE SaaS subscription is stated in the applicable Order or Supporting Material and begins on the date that HPE SaaS is made available to Customer ("SaaS Order Term").

4. **Access Rights.** During the applicable SaaS Order Term, Customer may access and use HPE SaaS in accordance with the applicable Supporting Material and this Agreement. Customer is responsible for complying with the terms of this Agreement and the Supporting Material. Customer is responsible for any and all use of HPE SaaS through Customer's credentials or any account that Customer may establish. Customer agrees to maintain the confidentiality of Customer's account, credentials, and any passwords necessary to use HPE SaaS. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify HPE.

5. **Usage Limitations.** HPE SaaS may be used only for Customer's internal business purposes and not for commercialization. Customer will not: (i) exceed any usage limitations identified in the Supporting Material; (ii) except to the extent expressly permitted in Supporting Material, sell, resell, license, sublicense, lease, rent, or distribute HPE SaaS or include HPE SaaS as a service or outsourcing offering, or make any portion of HPE SaaS available for the benefit of any third party; (iii) copy or reproduce any portion, feature, function, or user interface of HPE SaaS; (iv) interfere with or disrupt the integrity or performance of HPE SaaS; (v) use HPE SaaS to submit, send, or store Customer-provided SaaS Data that is obscene, threatening, libelous or otherwise unlawful or tortuous material, violates any third party's privacy rights, or infringes upon or misappropriates intellectual property rights; (vi) use HPE SaaS to disrupt or cause harm to a third party's system or environment; (vii) access HPE SaaS to build a competitive product or service; or (viii) reverse engineer HPE SaaS. Customer is responsible for complying with all terms of use for any software, content, service, or website it loads, creates, or accesses when using HPE SaaS.

6. **Payment terms.**
   a. **Prices and Taxes.** Prices will be as quoted in writing by HPE or, in the absence of a written quote, as set out on our website, customer-specific portal, or HPE published list price at the time an order is submitted to HPE. Prices are exclusive of taxes, duties, and fees unless otherwise quoted. If a withholding tax is required by law, please contact the HPE order representative to discuss appropriate procedures.
   b. **Invoices and Payment.** Customer agrees to pay all invoiced amounts within thirty (30) days of HPE's invoice date.

7. **Customer-provided SaaS Data.** Customer is solely responsible for the data, text, audio, video, images, software, and other content input into an HPE system or environment ("Customer-provided SaaS Data") during Customer's access or use of HPE SaaS. As between HPE and Customer, Customer is and will remain the sole and exclusive

owner of all right, title, and interest in and to all Customer-provided SaaS Data. Customer hereby provides to HPE all necessary rights to Customer-provided SaaS Data to enable HPE to provide HPE SaaS. HPE will use Customer-provided SaaS Data only as necessary to provide HPE SaaS, technical support, or as otherwise required by law.

8. **Personal Data.**
   a. If, in the course of providing HPE SaaS, HPE agrees in writing to process Customer Personal Data, HPE shall process such data only as mutually agreed, and in compliance with data protection legislation to which HPE is subject as a service provider and processor of Customer Personal Data.
   b. "Customer Personal Data" means personal data of which Customer or its affiliates is the controller and which HPE processes in the course of providing HPE SaaS. The terms "controller", "processor", "process", "processed", "processing", and "personal data" used in this Agreement shall be as defined by EU Directive 95/46/EC, unless otherwise defined by applicable data protection legislation.

9. **Data Security.** HPE implements technical and organizational measures to protect Customer-provided SaaS Data. The Supporting Material for each HPE SaaS describes the measures implemented for such HPE SaaS.

10. **HPE SaaS Performance and Operations.** HPE's ability to deliver HPE SaaS will depend on Customer's reasonable and timely cooperation and the accuracy and completeness of any information from Customer needed to deliver HPE SaaS.

11. **HPE SaaS Operations**. So long as during the SaaS Order Term, HPE does not materially degrade the functionality, as described in Supporting Material of HPE SaaS, HPE reserves the right: (i) to modify the systems and environment used to provide HPE SaaS; and (ii) to make any changes to HPE SaaS that it deems necessary or useful to maintain or enhance the quality or delivery of HPE's services to its customers, the competitive strength of or market for HPE's services, or HPE SaaS' cost efficiency or performance. HPE may use global resources, such as HPE affiliates or third parties in worldwide locations to provide HPE SaaS and perform its obligations.

12. **License Grant to Software in connection with HPE SaaS**. To the extent that HPE provides software in connection with HPE SaaS, HPE grants Customer a non-exclusive and non-transferable license to use the version or release of the HPE-branded software listed in the Order or the applicable Supporting Material (the "Licensed Software") during the SaaS Order Term. Unless otherwise stated in writing, Customer may only use the Licensed Software for internal purposes and not for further commercialization. Customer may make a copy or adaptation of the Licensed Software only for archival purposes or when it is an essential step in the authorized use of the Licensed Software. Customer agrees that it will not modify, reverse engineer, disassemble, decrypt, decompile, or make derivative works of any Licensed Software unless permitted by statute, in which case Customer will provide HPE with reasonably detailed information about those activities. For non-HPE branded software, the third party's license terms will govern its use. HPE may monitor and audit Customer use of the Licensed Software and compliance with any associated license terms and, if HPE makes a license management program available, Customer agrees to install and use it within a reasonable period of time. Customer may not sublicense, assign, transfer, rent, or lease the Licensed Software except as permitted in writing by HPE.

13. **Warranty:** HPE WILL PERFORM HPE SAAS BY QUALIFIED PERSONNEL AND IN A WORKMANLIKE MANNER CONSISTENT WITH THE SUPPORTING MATERIAL. TO THE EXTENT PERMITTED BY LAW, HPE DISCLAIMS ALL OTHER WARRANTIES. HPE DOES NOT WARRANT THAT HPE SAAS WILL BE UNINTERRUPTED OR ERROR FREE. IF HPE PROVIDES CUSTOMER WITH A FREE-OF-CHARGE SAAS ORDER TERM, INCLUDING BUT NOT LIMITED TO HPE SAAS PROVIDED ON AN EVALUATION OR "FREEMIUM" BASIS, HPE SAAS IS PROVIDED "AS IS" AND TO THE EXTENT PERMITTED BY LAW, HPE DISCLAIMS ALL WARRANTIES AND LIABILITY.

14. **Intellectual Property Rights.** No transfer of ownership of any intellectual property will occur under this Agreement. Customer grants HPE a non-exclusive, worldwide, royalty-free right and license to any intellectual property, including Customer-provided SaaS Data, that is necessary for HPE and its designees to perform HPE SaaS.

15. **Intellectual Property Rights Infringement**. HPE will defend and/or settle any claims against Customer that allege that an HPE-branded product or service as supplied under this Agreement infringes the intellectual property rights of a third party. HPE will rely on Customer's prompt notification of the claim and cooperation with our defense. HPE may modify the product or service so as to be non-infringing and materially equivalent, or we may procure a license. If these options are not available, we will refund to Customer the balance of any pre-paid amount for the affected HPE SaaS. HPE is not responsible for claims resulting from Customer-provided SaaS Data or from any unauthorized use of the products or services. This section shall also apply to Licensed Software identified as such in the relevant

Supporting Material except that HPE is not responsible for claims resulting from Customer-provided SaaS Data, customized configurations or designs (i) performed or provided by Customer or (ii) performed at Customer's direction. Customer will defend or indemnify HPE from and against third party claims arising from Customer-provided SaaS Data or customized configuration or designs (i) performed or provided by Customer or (ii) performed at Customer's direction.

16. **Limitation of Liability.** For violation of obligations and tort, HPE and its vicarious agents are liable without limitation in case of wilful conduct and gross negligence. The same applies to malicious concealment of a defect. As far as the violation on the part of HPE and its vicarious agents is not considered as wilful or gross negligent the liability is limited to a maximum amount up to the greater of 1 mio. € or the amount payable by the Customer to HPE for the relevant Order that is the subject of the claim for the twelve month period immediately preceding the act or omission giving rise to the claim. Any further liability is excluded, in particular such for consequential damages and loss of profit or data. This limitation does not refer to damages due to unauthorized use of intellectual property, life threatening, bodily injury or adverse health effects and claims under the Product Liability Act. In case of provision of personnel for work subject to Customer's supervision and direction, HPE shall only be liable if HPE had wilfully or gross negligently failed to choose such personnel in accordance with Customer's requirements which had been notified to HPE in advance. Any liability shall be excluded if the damage had also occurred in case of faultless selection of such personnel.Neither party will be liable for performance delays or for non-performance due to causes beyond its reasonable control, except for payment obligations. If HPE provides customer with a free-of-charge SaaS Order Term, including but not limited to HPE SaaS provided on an evaluation or "freemium" basis, HPE SaaS is provided "as is" and to the extent permitted by law, HPE shall not be responsible for any loss or damage to Customer, its customers, or any third parties caused by HPE SaaS or the Licensed Software that HPE makes available for Customer.

17. **Suspension**. HPE may suspend Customer's access and use rights to HPE SaaS where Customer breaches Sections 4, 5, 6, 7, or 12 of this Agreement or Customer's use of HPE SaaS is in violation of law and Customer fails to remedy the breach within a reasonable period after being notified by HPE in writing of the details. The suspension shall become effective after lapse of the cure period. Customer remains responsible for applicable fees from the date of suspension and throughout the suspension period, including usage and data storage fees. Customer will not be entitled to service credits, if any, during any suspension period.

18. **Termination**. Either party may terminate this Agreement on written notice if the other fails to meet any material obligation and fails to remedy the breach within a reasonable period after being notified in writing of the details. If either party becomes insolvent, unable to pay debts when due, files for or is subject to bankruptcy or receivership, or asset assignment, the other party may, if permitted by law, terminate this Agreement and cancel any unfulfilled obligations. HPE may terminate this Agreement where Customer's access and use rights are suspended pursuant to Section 17 or to comply with applicable laws or regulations. Any terms in the Agreement which by their nature extend beyond termination or expiration of the Agreement will remain in effect until fulfilled and will apply to both parties' respective successors and permitted assigns.

19. **Effect of Expiration or Termination**. Except for termination for cause in circumstances where HPE is at fault, termination of this Agreement shall not entitle Customer to any refund, and payment obligations are non-cancelable. Upon expiration or termination of a SaaS Order Term, except as otherwise provided in the Supporting Material:
    a. HPE may disable all Customer access to the applicable HPE SaaS, and Customer shall promptly return to HPE (or at HPE's request destroy) any Licensed Software provided with HPE SaaS; and
    b. HPE shall make available Customer-provided SaaS data in the format generally provided by HPE, subject to the terms of the applicable Supporting Material.

20. **General.** This Agreement, including its Exhibit 1, which is an integral part thereof, represents our entire understanding with respect to its subject matter and supersedes any previous communication or agreements that may exist. Modifications to this Agreement will be made only through a written amendment signed by both parties. The Agreement will be governed by the laws of the country of HPE or the HPE affiliate accepting the Order and the courts of that locale will have jurisdiction; however, HPE or its affiliate may bring suit for payment in the country where the Customer affiliate that placed the Order is located. Customer and HPE agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply. Claims arising or raised in the United States will be governed by the laws of the state of California, excluding rules as to choice and conflicts of law.

Signed for HPE by:

……
[Insert signature]

……
[Insert name and business title]

HPE Entity:……

Date: ……

Signed for Customer by:

……
[Insert signature]

……
[Insert name and business title]

Customer Entity:……

Date: ……

Exhibit 1 – DATA PROTECTION

A: Data Protection Provisions

1. To the extent HPE has access to Customer´s personal data for performing Software-as-a-Service (hereinafter "SaaS"), the Parties agree to apply the terms described below. HPE shall apply those technical and organizational measures required by the exhibit to § 9 BDSG as set out below under section B.

   Provisions pursuant to Sections 9, 11 of the German Federal Data Protection Act (BDSG):

2. **Underlying SaaS Contract.** The terms of the agreement on commissioned data processing are based upon the SaaS contract concluded between the Parties, including the appendixes describing the SaaS services (SaaS data sheets) (the "Contract"). On the basis of the aforementioned Contract, HPE will process the Customer's personal data. The Contract defines the scope, nature, and purpose of the collection, processing and/or use of personal data by HPE, the type of personal data to be processed and the persons affected by the handling of personal data. The Customer may also provide additional written instructions. The duration of the commissioned data processing will be governed by the Contract.

3. **Correcting, blocking, and deleting data.** HPE may only correct, delete or block data processed within the scope of the Contract in accordance with the instructions provided by the Customer. If a person asks HPE for information about his/her data or requests that HPE correct or delete his/her data, HPE shall immediately forward the request to the Customer.

4. **Obligations of HPE.** To ensure proper processing of personal data, HPE will only use personnel who have entered into confidentiality agreements pursuant to Section 5 of the BDSG. If the security measures implemented by HPE do not satisfy the requirements of the Customer, the Customer will notify HPE immediately. Any errors or irregularities that are identified by the Customer when checking the results, and brought to HPE's attention, will be immediately rectified by HPE. HPE will process personal data and other operating data belonging to the customer only in accordance with the instructions provided by the Customer. HPE will not use the data transmitted for data processing for any other purpose, nor will HPE retain this data for any longer than required by the Customer, save to the extent required by legal retention periods. Copies or duplicates must not be created without informing the Customer. If HPE believes that an instruction from the Customer violates data protection legislation, HPE must notify the Customer. This duty to notify will not include a comprehensive legal review. Subcontracts may only be awarded to subcontractors following written consent by the Customer. A Customer's consent may only be withheld if the Customer has a material reason for doing so. The Customer's consent will be deemed to have been given with respect to subcontractors named by HPE prior to the conclusion of the Contract or which are regularly used by HPE to provide standardized services. If a subcontractor is a company within HPE's corporate group and is based in the European Union (EU) or the European Economic Area (EEA) or a safe third country, a subcontract may be awarded to the subcontractor without the prior written consent of the Customer. Irrespective of this, HPE will always be obliged to exercise due caution when choosing subcontractors and to inform the Customer accordingly. Furthermore, HPE must ensure that the data processing provisions agreed with the Customer also apply to all subcontracts awarded to subcontractors. If a subcontractor is operating outside the European Union (EU) or European Economic Area (EEA), an adequate level of data protection must be established pursuant to Sections 4b and 4c of the BDSG. To this end, the Customer hereby authorizes HPE to execute a controller to processor EU Model Contract (C (2010) 593) on its behalf to cover the transfer of any Customer personal data which originates from the EEA to any HPE Affiliate supporting the SaaS or Professional Services and being located in a country which does not have a finding of adequacy pursuant to Article 25(6) of Directive 95.46/EC (the "Model Contract").

5. HPE will immediately inform the Customer of any incidents that must be reported pursuant to Section 42a of the BDSG, any serious operational malfunctions, and any suspected privacy violations or other irregularities that arise while

processing the Customer's data. HPE has appointed a competent and reliable data protection officer pursuant to Section 4f of the BDSG.

6. **Control rights of the Customer.** The Customer or a representative appointed by the Customer has a right of control with regard to proper processing of personal data and other operational data processed on behalf of the Customer. The rights of control will be exercised in consultation with HPE. HPE is obliged to assist the Customer in such controls and any controls of the competent authorities. These controls must be carried out in consideration of the business processes and HPE's need for security and confidentiality. The control of standardized services will be performed by controlling the test documents professionally created and submitted by HPE. HPE is also obliged to apply the control rights of the Customer to the subcontractors of HPE tasked with processing the Customer's data.

7. **Deletion of data and return of data carriers.** After completion of the contractual work or earlier if requested by the Customer - at the latest upon termination of the Contract - HPE must return to the Customer all documents, processing results, usage results, and data sets that relate to the contractual relationship, or to destroy them in a manner compatible with data protection legislation following prior approval by the Customer. The same will apply to test material and rejected material. The manner in which data is deleted must be demonstrated upon request. HPE must retain any documentation serving as proof of commissioned data processing and proper data processing beyond the end of the Contract in accordance with the respective retention periods. To ease the burden on HPE, HPE can choose to hand over such documentation when the Contract terminates.

B. Technical and Organizational Measures pursuant to Section 9 of the German Federal Data Protection Act (BDSG) and the Annex to this Act

The following technical and organizational measures will be implemented by HPE and subject to technical advances and further development in accordance with Section 3 of this DPSA. In this respect, HPE will be allowed to implement adequate alternative measures. The security level of the defined measures must not be compromised. Significant changes must be documented. If authorizations to access systems or applications are necessary to perform the services agreed in the Commercial Agreement, HPE may only award such authorizations, for the intended purpose and to the extent required, to persons tasked with the processing related to the Commercial Agreement. In the event that HPE needs to telework in order to perform certain activities, HPE will use appropriate measures to ensure the necessary level of protection and security. HPE will inform Customer of such measures upon request. HPE will also ensure that appropriate controls are implemented.

1. **Entry Control.** Entry to buildings, rooms, and facilities in which Customer Personal Data is collected, processed or used, will be restricted to authorized persons. To ensure secure entry to company buildings and rooms, and the identification of authorized persons, HPE will deploy and use effective and appropriate access controls such as electronic smart cards, door locking systems, and technical surveillance equipment. Such controls will be at the individual person level as appropriate. Furthermore, appropriate and effective surveillance equipment such as video and alarm systems will be installed.

2. **Access Control.** In order to obtain access to HPE's technical systems, applications and net-works, a password-protected user master record (known as the personal user account) must be set up. The authorized user will then use this account to authenticate him-self/herself to the system or application. When leaving a computer, the user must log off accordingly. When assigning a password, user authentication must be sufficiently secure. The user account must be formally requested, approved by the relevant supervisor, and the assignment documented. HPE has outlined the design, use, and personal scope of the password in a password policy whose compliance is supported technically. Applications and communication connections will force re-authentication when certain thresholds are reached (maximum session duration, failed logons, etc.). Any systems vulnerable to attack by malicious software will be equipped with the latest protection.

3. **Authorization Control.** HPE will grant access authorizations on a "need-to-know" and "need-to-do" basis (lowest possible rights). Examples include access authorizations for task-related authorization schemes, user profiles, and functional roles. An access authorization will be sought on the basis of the role scheme and approved by the relevant

supervisor. Additional control instances will be integrated into the approval process. For technical access security, HPE will use recognized security systems such as RACF, Active Directory, etc. Existing user accounts will be checked periodically and deleted or changed in the event that a user's tasks change. The responsibility for user accounts must be clearly assigned; representations are defined allowed in the current policies.

4. **Disclosure Control.** Technical (protection when saving and transferring data) HPE will ensure the integrity of Customer Personal Data stored and disclosed within the data processing systems and applications through the use of plausibility checks and/or verification procedures. The confidentiality of Customer Personal Data outside HPE's area of responsibility (for example, third-party networks and radio networks) will be ensured through authentication and/or encryption. Remote access to networks that house Customer's systems and applications will be encrypted and only granted after authentication. Several factors will be associated with particularly sensitive data (for example, password and hardware token). Networks that house Customer's systems and applications will be separated from other networks through the use of proxies, firewalls "with stateful inspection", and a network address translation (NAT). In addition to Secure Socket Layer (SSL) encryption and the use of VPN technology, secure Internet communication will be achieved through the use of firewall systems and continuously updated virus software. Data carriers will be transported in encrypted form only.

5. **Receiver control (traceability of planned transfers).** The purpose, type, origin and destination of each automatic data exchange with third-party systems and networks will be documented.

6. **Input Control.** In general, HPE will log all data input and output activity undertaken by users and administrators using the systems and applications, and will check this data for irregularities on a regular basis. The logs will be archived in accordance with the content and/or statutory requirements. Alternatively, they will be deleted once they have fulfilled their purpose or they will be blocked against further processing. Predominantly automated reconciliation procedures and controls will ensure effective processing. Log data will be stored securely and the use of audit tools will be limited to authorized users.

7. **Task Control.** HPE will process the entrusted data only in accordance with the contractually agreed instructions received from Customer. Control measures will be defined in consultation with Customer and then technically or organizationally incorporated into the operations. HPE will only engage the services of subcontractors in accordance with the requirements of the contractual provisions.

8. **Availability Control.** HPE will use off-site backup data centers for this purpose. Systems will be protected against attacks from outside. The availability of data and systems in data centers will be ensured through appropriate measures such as system redundancy, battery backup against power outages, air conditioning, and protection against other harmful environmental agents and sabotage. The relevant facilities will be maintained and tested on a regular basis, in accordance with manufacturer specifications. Archive data will be generated in accordance with the respective applicable requirements. To ensure a reliable recovery in the event of a serious malfunction, flow definitions for continuity plans will be developed, tested on a regular basis, and kept highly available.

9. **Separation Control.** Systems and applications will be geared specifically towards purpose-specific and Customer-separate processing. There will be a functional separation between production systems and test systems. The test data in production systems may only be used following consultation with Customer, and only if the test system's security is comparable with that of the production system. Tests will not reduce the level of protection in terms of confidentiality, integrity or availability of Customer Personal Data.