

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

HPE CUSTOMER TERMS - SOFTWARE-AS-A-SERVICE

1. **Parties.** These terms represent the agreement (“**Agreement**”) that governs the purchase of SaaS from the Hewlett Packard Enterprise entity identified in the signature section below (“**HPE**”) by the Customer entity identified below (“**Customer**”).
2. **Definitions.**
 - a. “**HPE Software**” means the on-premise version of an HPE software product, if any, delivered as a service and as identified in a data sheet and/or Statement of Work (“**SOW**”) (either or both “**Supporting Material**”).
 - b. “**Order**” means the accepted order including any supporting material which the parties identify as incorporated either by attachment or reference (“**Supporting Material**”). Supporting Material may include (as examples) standard or negotiated service descriptions, data sheets and their supplements, and statements of work (SOWs), and may be available to Customer in hard copy or by accessing a designated HPE website.
 - c. “**SaaS**” means the online software-as-a-service solution that HPE provides, including support, and related professional services as described in the Supporting Material and other exhibits or attachments that are made a part of this Agreement.
3. **Overview.** SaaS may be used only for Customer’s internal business purposes and not for commercialization. The SaaS term is in the relevant Supporting Material or HPE quotation (the “**SaaS Term**”). If Customer previously purchased a perpetual license to HPE Software, the price of SaaS shall reflect such purchase and such pre-existing license shall be deemed to be used in relation to SaaS. During the SaaS Term, Customer may not use such HPE Software installed on Customer infrastructure except in connection with receipt of SaaS.
4. **Scope and Order Placement.** These terms may be used by Customer either for a single Order or as a framework for multiple Orders. In addition, these terms may be used on a global basis by the parties’ “Affiliates”, meaning any entity controlled by, controlling, or under common control with a party. The parties can confirm their agreement to these terms either by signature where indicated at the end or by referencing these terms on Orders. Affiliates participate under these terms by placing orders which specify product or service delivery in the same country as the HPE Affiliate accepting the Order, referencing these terms, and specifying any additional terms or amendments to reflect local law or business practices.
5. **Order Arrangements.** Customer may place orders with HPE through our website, customer-specific portal, or by letter, fax or e-mail. Where appropriate, orders must specify a delivery date. If Customer extends the delivery date of an existing Order beyond ninety (90) days, then it will be considered a new order.
6. **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. HPE will charge separately for reasonable out-of-pocket expenses, such as travel expenses incurred in providing professional services.
7. **Invoices and Payment.** Customer agrees to pay all invoiced amounts within thirty (30) days of HPE’s invoice date. HPE may suspend or cancel performance of open Orders or services if Customer fails to make payments

Agreement Number(s) where required:

HPE:.....

Customer:.....

Effective Date (if applicable):.....

Term Length (if applicable):.....

when due.**8. Dependencies.** HPE's ability to deliver SaaS will depend on Customer's reasonable and timely cooperation and the accuracy and completeness of any information from Customer needed to deliver the services.

- 9. Change Orders.** We each agree to appoint a project representative to serve as the principal point of contact in managing the delivery of SaaS and in dealing with issues that may arise. Requests to change the scope of SaaS will require a change order signed by both parties.
- 8. SaaS Performance.** SaaS is consistent with generally recognized practices and standards for software-as-a-service.
- 9. Remedies.** This Agreement states all remedies for warranty claims. HPE does not warrant that SaaS will be uninterrupted or error free. To the extent permitted by law, HPE disclaims all other warranties.
- 10. 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 that is necessary for HPE and its designees to perform the ordered services. If deliverables are created by HPE specifically for Customer and identified as such in Supporting Material, HPE hereby grants Customer a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally.
- 11. 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 amount paid for the affected product in the first year or the depreciated value thereafter or, for support services, the balance of any pre-paid amount or, for professional services, the amount paid. HPE is not responsible for claims resulting from any unauthorized use of the products or services. This section shall also apply to deliverables identified as such in the relevant Support Material except that HPE is not responsible for claims resulting from deliverables content or design provided by Customer.
- 12. Confidentiality.** Information exchanged under this Agreement will be treated as confidential if identified as such at disclosure or if the circumstances of disclosure would reasonably indicate such treatment. Confidential information may only be used for the purpose of fulfilling obligations or exercising rights under this Agreement, and shared with employees, agents or contractors with a need to know such information to support that purpose. Confidential information will be protected using a reasonable degree of care to prevent unauthorized use or disclosure for 3 years from the date of receipt or (if longer) for such period as the information remains confidential. These obligations do not cover information that: i) was known or becomes known to the receiving party without obligation of confidentiality; ii) is independently developed by the receiving party; or iii) where disclosure is required by law or a governmental agency.
- 13. Personal Information.** Customer and HPE shall comply with their respective obligations under applicable data protection legislation as a controller and processor, respectively. Customer shall remain the controller of Customer Personal Data (as defined in the Exhibit) at all times. Exhibit "SaaS Data Protection Regulations" forms part of this Agreement and takes precedence over any conflicting terms herein or in any Supporting Material.
- 14. Security.** Information about SaaS' security controls are provided at the hp.com website or can be otherwise provided at Customer's request.

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

- 15. Global Trade compliance.** If Customer exports, imports or otherwise transfers products and/or deliverables provided under these terms, Customer will be responsible for complying with applicable laws and regulations and for obtaining any required export or import authorizations. HPE may suspend its performance under this Agreement to the extent required by laws applicable to either party.
- 16. Limitation of Liability.** HPE's liability to Customer under this Agreement is limited to the greater of \$1,000,000 or the amount payable by Customer to HPE for the relevant Order. Neither Customer nor HPE will be liable for lost revenues or profits, downtime costs, loss or damage to data or indirect, special or consequential costs or damages. This provision does not limit either party's liability for: unauthorized use of intellectual property, death or bodily injury caused by their negligence; acts of fraud; willful repudiation of the Agreement; nor any liability which may not be excluded or limited by applicable law.
- 17. Disputes.** If Customer is dissatisfied with SaaS and disagrees with HPE's proposed resolution, we both agree to promptly escalate the issue to a Vice President (or equivalent executive) in our respective organizations for an amicable resolution without prejudice to the right to later seek a legal remedy.
- 18. Force Majeure.** Neither party will be liable for performance delays or for non-performance due to causes beyond its reasonable control, except for payment obligations.
- 19. 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 terminate this Agreement and cancel any unfulfilled obligations. 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.
- 20. Rescheduling.** Customer has the one-time right to reschedule the Order start date without charge (for a date that is no more than three (3) months after the originally scheduled start date) upon no less than three (3) business days' written notice prior to the date that delivery is scheduled to begin. Customer shall forfeit any days that are rescheduled with less than three (3) business days' notice.
- 21. Effect of Termination.** Except for termination for cause, the termination of this Agreement shall not entitle Customer to any refund.
- 22. Order of Precedence.** To the extent that the terms of this Agreement conflict with other terms in any other agreement between Customer and HPE, the terms in this Agreement shall control as to SaaS.
- 23. General.** This Agreement represents our entire understanding with respect to its subject matter and supersedes any previous communication or agreements that may exist. Modifications to the 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.

EXHIBIT - SAAS DATA PROTECTION REGULATIONS GERMANY (Version January 1, 2013)

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

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 in subsection 1.1. HPE shall apply those technical and organizational measures required by the exhibit to § 9 BDSG as set out in subsection 1.2 below.

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

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.

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.

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”).

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.

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

Agreement Number(s) where required:

HPE:.....

Customer:.....

Effective Date (if applicable):.....

Term Length (if applicable):.....

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.

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.

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

The contractual partners have agreed the technical and organizational measures prior to the Contract being awarded. The technical and organizational measures will be subject to technical advances and further development. 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 Contract, HPE may only award such authorizations, for the intended purpose and to the extent required, to persons tasked with the processing related to the Contract. 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 the Customer of such measures upon request. HPE will also ensure that appropriate controls are implemented.

Entry Control. Entry to buildings, rooms, and facilities in which 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. The data centers of HPE are certified in accordance with ISO 27001 and ISAE 3402, or, appropriate processes and standards have been implemented.

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.

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.

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

Disclosure Control. Technical (protection when saving and transferring data) HPE will ensure the integrity of 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 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 the 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 the 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.

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.

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.

Task Control. HPE will process the entrusted data only in accordance with the contractually agreed instructions received from the Customer. Control measures will be defined in consultation with the 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.

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.

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 the 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 personal data.

Signed for Hewlett-Packard GmbH (HPE):
[Insert signature]

By:
[Insert name]

Title:
[Insert signatory's business title]

Agreement Number(s) where required:

HPE:.....

Customer:.....

Effective Date (if applicable):.....

Term Length (if applicable):.....

HPE Entity:

Date:
[Insert date]

Signed for Customer:
[Insert signature]

By:
[Insert name]

Title:
[Insert signatory's business title]

Customer Entity:

Date:
[Insert date]