BMC INNOVATION SUITE DATA PROCESSING AGREEMENT

PREAMBLE

This standard Data Processing Agreement on the commissioned processing of personal data ("**DPA**") forms an integral part of the Order this DPA is attached to. Capitalized terms not defined herein shall have the meanings given to them in the BMC Innovation Suite and Applications Agreement (**"Agreement**"). BMC and Customer may be referred individually as to a "**Party**" or collectively as to the "**Parties**". This DPA shall commence on the Order Date (hereinafter referred as the "**Effective Date**").

In the course of providing the Services to Customer pursuant to the Agreement, BMC may come to have access to Personal Data as may be submitted into the Services by Customer as Customer Data. BMC agrees to comply with the following provisions with respect to any Personal Data submitted into the Services as Customer Data. This DPA does not govern the processing of Customer Data by Third Party Publishers and/or through the use by Customer of Third Party Applications running on the Platform Services.

For the purposes of this DPA, "**Personal Data**", "data processor", "data controller", "processing" have the meaning specified for each term respectively in European Directive 95/46/EC and/or the EU Regulation 2016/679 as applicable (hereinafter referred to as "**European Data Protection Laws**") where such data is submitted by or for Customer into the BMC systems.

1. **BMC OBLIGATIONS.**

1.1 This DPA applies to the transfer and processing of data for the purpose of processing Customer Data in accordance with European Data Protection Laws. BMC and Customer acknowledge that with regard to the Services, Customer is the 'data controller', BMC is the 'data processor' and both parties shall fulfill their respective legal obligations.

1.2 BMC will not access Customer Data except as required to provide the Services or at Customer's specific request. BMC has implemented and will maintain procedures to logically segregate Customer Data.

1.3 BMC shall process and use Personal Data for the following purposes as further defined in Annex 1 to this DPA:

(a) to provide the Services, to prevent or address service or technical problems, or upon Customer's request in connection with a customer support matter;
(b) processing initiated by Customer's Users in their use of the Services.

Additionally, as set forth in the DPA, BMC shall not disclose Personal Data except as expressly permitted in writing by Customer or where required by law. Unless prohibited from doing so by a law enforcement authority or agency, BMC shall notify Customer promptly with prior notice of any such compelled disclosure, in accordance with Rule 12-B of the BCR Policy.

1.4 BMC shall process and use Personal Data in accordance with the Customer's instructions as set forth in the Agreement and this DPA. The following are deemed as instructions by Customer to process Personal Data:

(a) processing necessary for the exercise and performance of Customer's rights and obligations under the Agreement and this DPA respectively; and
(b) processing initiated by the Customer's users (hereinafter referred as "**Customer Users**") in their use of the Services.

Personal Data may be processed or used for another purpose only with the prior written consent of Customer. For clarity, BMC shall not collect Personal Data on behalf of Customer.

1.5 BMC shall treat Personal Data as Confidential Information and shall comply with European Data Protection Laws applicable to BMC as a Data Processor in providing the Services.

1.6 **Binding Corporate Rules**. BMC adheres to its Controller and Processor Binding Corporate Rules Policy (the "BCR") approved by European data protection authorities with respect to compliance with European data protection laws. The BCR policy is incorporated into a BMC corporate wide policy, requiring all BMC entities, employees and third party providers to comply with and respect the BCR policy which is governing the collection, use, access, storage and transfer of Personal Data among BMC entities and third-party sub-processors. Customer agrees to rely upon the BCR as providing adequate safeguards in regards to EU Data Protection Laws and provisions contained in the Introduction, Part III and IV of the BCR are incorporated by reference and are an integral part of this DPA. A copy of the BCR can be found at: http://www.bmc.com/legal/data-privacy-binding-corporate-rules.html. Customer agrees that Personal Data may be processed by the BMC Affiliates provided that BMC and its Affiliates are and remain contractually bound by the BCR. BMC represents that its Affiliates are and shall for the duration of the DPA remain contractually bound by and comply with the requirements of the BCR. The details of the BCR approval of BMC Software are available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

1.7 Where Customer, based upon European Data Protection Laws, is obliged to provide information to a data subject about the collection, processing or use of its Personal Data, then to the extent the Customer does not have access to that information in its use of the Services or otherwise, BMC shall assist Customer in making reasonably required information available, provided that (i) Customer has instructed BMC in writing to do so, and (ii) Customer reimburses BMC for any reasonable costs arising from any such assistance. For the avoidance of doubt, Customer shall be solely responsible for communicating directly with data subjects.

1.8 If BMC receives any complaint, notice, or communication that relates to BMC's processing of Personal Data submitted into the Services by Customer or either party's compliance with European Data Protection Laws in connection with Personal Data submitted into the Services by Customer, to the extent legally permitted, BMC shall promptly notify Customer and, to the extent applicable, BMC shall provide Customer, with reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

1.9 BMC shall promptly inform Customer about any of the following: (i) infringements of European Data Protection Laws that relate to Personal Data submitted into the Services by Customer that may come to its attention; (ii) actual or reasonably suspected unauthorized access to or disclosure of Personal Data submitted into the Services by Customer of which BMC becomes aware; or (iii) material violations of the provisions of this DPA by BMC or Sub-Processors, as defined below.

1.10 BMC shall implement appropriate organizational and technical protection measures as set out in Annex 2 to this DPA. BMC regularly monitors compliance with these measures.

1.11 Notwithstanding the provisions of 1.9 above, Customer acknowledges that BMC may, as a part of ongoing system maintenance and development, change its appropriate organizational and technical protection measures. BMC shall not provide for protection measures that deliver a level of security protection that is materially lower than that provided as at the DPA Effective Date and will be maintained by BMC at all times throughout the Term of the Agreement and this DPA.

1.12 BMC shall ensure that all personnel of BMC granted access to Personal Data have executed written confidentiality obligations with a level of protection as required under the Agreement. The obligation to treat Personal Data pursuant to such confidentiality obligations shall survive the termination of the employment, and only so long as such Personal Data is considered Confidential Information. Personal Data may be made available only to personnel that require access to such Personal Data for the performance of this DPA.

2. **RIGHTS AND OBLIGATIONS OF CUSTOMER.**

2.1 Customer as applicable has the right to give instructions to BMC for the processing of Personal Data, as provided for and within the limits of this DPA and the Agreement. Customer may provide BMC with such instructions in writing, or the Customer may provide BMC with such instructions via online authorization tools via the Services. In addition, Customer acknowledges that by virtue of using the Services, it gives BMC instructions to process and use Personal Data to provide the Services and prevent or respond to technical or service problems in accordance with this DPA.

2.2 Customer is responsible for compliance with applicable European Data Protection Laws in its use of the Services, including those pertaining to transfers of or access to Personal Data initiated by the Customer's Users.

3. **SUB-PROCESSORS OF PERSONAL DATA.**

3.1 Customer and BMC agree that "**Subprocessor**" means any data processor engaged by BMC that processes Personal data on behalf of Customer that may be an affiliate of BMC or a third party engaged by BMC or a BMC Affiliate. Customer acknowledges and agrees that BMC may engage its affiliates or third parties as Subprocessors to assist in the provision of customer support only, including access to Personal data, in connection with the Services. The Subprocessors only have access to Customer Data to the extent Customer grants such access to BMC and its Subprocessors. A full list of all Subprocesors (including BMC Affiliates and third party Subprocessor) as of the Effective Date of this DPA is provided in Annex 3 to this DPA. Any additions or amendments to this list will be notified to customer, via email to the email address stated in the Order.

3.2 Sub-Processors of Personal Data will be subject to data protection obligations at least equivalent to those contained in the Agreement and this DPA, and such Sub-Processors shall be obliged (i) to comply with European Data Protection Laws and (ii) to provide at least the same level of privacy protection as is required by this DPA and the Agreement.

4. **AUDIT RIGHTS.**

BMC obtains annual third party security audits of the BMC Subscriptions Services detailing BMC's compliance with the industry information security standard and data protection security ("**Security Audit**") and agrees it will provide disclosure of a copy of its

most then-recent Security Audit upon Customer's request, no more than annually, provided that Customer agrees to enter into a non-disclosure agreement with BMC.

5. **RIGHTS IN THE DATA AND DATA CARRIERS; CORRECTION, DELETION AND RETURN.**

5.1 The Customer maintains all rights in Personal Data and in all copies thereof.

5.2 To the extent Customer's Users cannot correct, delete or block Personal Data in their use of the Service, BMC shall use reasonable efforts to comply with a reasonable request from Customer within a reasonable period of time.

5.3 Upon request by Customer made within 30 days after the effective date of termination of the Order, BMC will make available to Customer for download a file of Customer Data in comma separated value (.csv) format or database backup format. After such 30-day period, BMC shall have no obligation to maintain or provide any Customer Data and will thereafter, unless legally prohibited delete Customer Data from the BMC Services.

6. **MISCELLANEOUS.**

6.1 This DPA begins upon the Effective Date and shall be in force and effect until the Order has been terminated or expires. In the event that after termination of the Order processing of Personal Data by BMC is necessary for the purpose of the Agreement or provided by law, *e.g.*, regarding the return of Personal Data, this DPA shall continue to apply until the completion of the purpose or return, as applicable.

6.2 Any BMC obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this DPA.

6.3 In the event of a contradiction between the Agreement and this DPA with respect to the processing of Personal Data contemplated hereunder, this DPA shall prevail.

Annex 1 - Details of the Data Processing

Categories of Personal Data and concerned Data Subjects

(a) Data Subjects

The Personal Data concern the following categories of data subjects (please specify):

- Customers
- Prospective Customers
- Employees
- Suppliers

(b) Categories of Data

The Personal Data concern he following categories of data (please specify):

- Personal master data (name, address, title, degree, date of birth)
- Contact details (telephone number, mobile phone number, email address, fax number)
- Contractual master data
- Customer history

Annex 2 - Technical and Organisation Security Measures

1. **Access control to premises and facilities to prevent unauthorized persons from gaining access to data processing systems for processing or using Personal Data.**

BMC has deployed the following measures to control access to systems and data:

- BMC has an identity management system fully integrated with BMC human resources system providing full lifecycle management for BMC Users Accounts and access to data. BMC User Accounts can only be requested and authorized for current employees and all managed accounts and access are revoked immediately upon termination of employment of such BMC user account, including disconnection of active remote access sessions; and
- BMC User Accounts are generated on a per-individual basis and not shared.

BMC, in conjunction with data center partner, Equinix, has deployed the following measures to protect and control a secured access to its facilities and data center:

- Access to BMC's production and disaster recovery ("DR") data centers is securely controlled and monitored by several layers of security implemented by Equinix.
    - All incoming Power and Telco man holes security locked down and diverse;
    - Speed reduction humps approaching the gate, embankment below power systems;
    - Bollard crash protection and Security controlled access;
    - Number plate recognition cameras;
    - Entire perimeter on zoned trembler wire system linked to CCTV and Security;
    - Additional crash protection fence facing the road;
    - Infra-red motion detectors, pressure pads on embankments;
    - Site cameras with night vision and motion detection;
    - Proximity card and finger print bio-metric access; and
    - CCTV cameras in every module on entry, exit and corridors.
- Keys and/or combination locks are not used for securing the data centers.
- No entry to site without approved Change Control, photo ID card and SC Clearance.
- Guests to Equinix data centers must be escorted by authorized Equinix personnel according to Equinix internal policies. Logical and physical securities measures are deployed at the data center located in the United Kingdom require that all guests must be first authorized by BMC management, and subsequently approved by Equinix data center management, prior to the visit.

2. Access control to systems to prevent data processing systems from being used without authorization.

BMC has deployed the following measures to provide a secured access to systems:

- For purposes of supporting BMC Innovation Suite, BMC user accounts are required in order to access any BMC Innovation Suite environment. Access must be requested per user and approved by BMC management.
- Logical access to the BMC Innovation Suite environments requires network connectivity from a BMC corporate network.

3. Access control to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

BMC has deployed the following measures to ensure that access to the BMC Innovation Suite systems is only available for BMC authorized personnel:

- Unique usernames and passwords are required for BMC personnel to access the BMC Innovation Suite systems, with mandatory complexity requirements, password history, and change frequency.
- BMC has deployed measures to ensure that its support personnel takes full accountability for the Personal Data processed on behalf of Customer in the format of login banner ("**Login Banner**") which outlines to the individual login into its BMC User Account (i) what are the acceptable use policy for support activities and (ii) prohibits reading, copying, modification, or removal of Personal Data that is entrusted to a support person and (iii) require the Support person to accept the terms ascribed into the Login Banner in order to login into their BMC User Account.

  The Login banner includes the following:
  "By completing the log-in process, you are acknowledging and consenting to proper use of BMC computing resources as specified in this notice and in applicable BMC policies, as well as agreeing that customer data entrusted to you for the express and specific purpose stated by the customer will not be processed, read, altered, disclosed, copied, modified, shared,

transferred, deleted or removed for purposes outside of the stated specific purpose without the explicit written consent of the customer."

- BMC maintains a confidential information protection policy that outlines data handling practices based on classification for which all BMC employees must comply to.
- BMC user accounts are required to access the BMC Innovation Suite system used for support and such accounts are only granted by BMC management approval.

4. **Disclosure control to ensure that Personal Data cannot be read, copied, altered, or removed without authorization during electronic transfer or transfer or transport or while being recorded onto data storage media, and that it is possible to check and establish to which parties Personal Data are to be transferred by means of data transmission facilities.**

   BMC has deployed security measures to ensure that Personal Data is fully encrypted, using AES 256, in transport as it moves from the Customer site to the BMC Innovation Suite data centers.

   Customer communication to any BMC Innovation Suite system requires the use of an encrypted transmission channel, including but not limited to, HyperText Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), Internet Protocol Security Virtual Private Network (IPSec VPN).

5. **Input control to ensure that it is possible to after-the-fact check and establish whether Personal Data has been entered into, altered, or removed from data processing systems, and if so, by whom.**

   BMC has implemented controlled and secured logging procedures applicable to the BMC Innovation Suite systems where the Personal Data resides. Logging provides full accountability for actions taken against Personal Data and by whom within the BMC Innovation Suite organization. Logs are retained for a period of at least consecutive six (6) months.

6. **Job control to ensure that personal data processed on behalf of others are processed strictly in compliance with the Data Controller's instructions.**

   As set forth in the DPA, BMC shall process Personal Data in accordance with the instructions of Customer while providing the BMC Services and in compliance with the Customer's lawful and explicit instructions.

7. **Availability control to ensure that Personal Data are protected against accidental destruction or loss.**

   BMC has a 24/7 network and security operations centers (NOC/SOC) to respond to network and security related incidents and provide continuous monitoring of BMC Innovation Suite systems. BMC has a variety of security tools implemented to protect its environment and data entrusted to it, including but not limited to, intrusion prevention services (IPS), anti-virus, application heuristic analysis (sandboxing), endpoint encryption, security information and event management (SIEM), rogue system detection (RSD), and web content filtering.

   BMC maintains a formal incident response and cyber crisis plan that includes standard actions and engagement for incident handling that includes notification to the customer and authorities.

8. **8. Segregation control to ensure that data collected for different purposes can be processed separately.**

   BMC has deployed the following measures:

   - Permissions and access control lists within BMC Innovation Suite environment allow logically segregated processing of personal data;
   - Access control within the BMC Innovation Suite environment is restricted and isolated so usage activities for one BMC customer cannot be viewed or accessed by another BMC customer.
   - BMC support access is restricted by role-based access control lists that segregate by job role. For example, Operations personnel can access Customer systems, but have no access to the database servers where Personal Data is stored.

Annex 3 - BMC Customer Support Services: BMC Affiliates and Third Parties entities engaged in Processing Customer Data

Entity Name	Entity Type	Entity Country
BMC Affiliates		
BMC Software, Inc., 2101 CityWest Boulevard, Houston, Texas 77042	Affiliate	USA
BMC Software Melbourne VIC Level 10 Twenty8 Freshwater Place, Melbourne VIC 3006	Affiliate	Australia
BMC Software Limited, E2 Eskdale Road, Winnersh, Wokingham, Berkshire, RG41 5TS, United Kingdom	Affiliate	United Kingdom
BMC Software 10431 Morado Circle, Avalon Bldg 5 Austin, TX 78759	Affiliate	USA
BMC Software 8401 Greensboro dr, suite 100 Greensboro Corp Center, McLean VA 22102	Affiliate	USA
BMC Software 6200 Stoneridge Mall Road Suite 200 Pleasanton, CA 94588	Affiliate	USA
BMC Software Ballymoss House Carmanhall road, Foxrock Dublin, Ireland	Affiliate	Ireland
BMC Software, Wing 1, Tower 'B', Business Bay, Survey No. 103, Hissa No. 2, Airport Road, Yerwada, Pune, Maharashtra 411006	Affiliate	India
BMC Software 600 North Bridge Road, #20-01/10 Park view Square	Affiliate	Singapore
Third Parties entities		
Nityo Infotech Services Pvt Ltd., 329/330, Laxmi Mall, Laxmi Industrial Estate, New Link Road, Andheri, Mumbai 400 053, India	Outsourcer	India
YIDATEC Co. Ltd, HeYi Building 10F, 6Aixian St., Hi-Tech Park, Dalian, China 116023	Outsourcer	China
VYOM Labs – Aditi Smruddhi, Survey No. 173/4, 4th floor, Baner, Pune-411 045	Outsourcer	India

BMC's Subcontractor (Equinix) Entities Operating Data Centers**

Entity Name	Entity Type	Entity Country
Equinix, Science Park 610, 1098 XH Amsterdam, Netherlands	Datacenter	Netherlands
Equinix, Luttenbergweg 4, 1101 EC Amsterdam, Netherlands	Datacenter	Netherlands
Equinix, Telfordstraat 3, 8013 RL Zwolle, Netherlands	Datacenter	Netherlands

***BMC Subcontractor's (Equinix) is used to store all data from Customer but does not process any of the Customer Personal Data.*