Data Processing Agreement

This Data Processing Agreement ("**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 Order or the BMC Cloud Services Master Agreement referenced in the Order. This DPA shall commence on the Order Date (hereinafter referred to as the ("**Effective Date**").

1. **GENERAL DEFINITIONS**.
"**Agreement**" is an agreed written or electronic document, that sets the framework terms under which BMC will supply BMC Products and/or BMC Services to Customer and Customer will receive them.
"**Binding Corporate Rules**" or "**BCR**" are BMC's Controller and Processor Binding Corporate Rules Policy available at www.bmc.com.
"**BMC Products**" is the specific supply of a license agreed under an Order.
"**BMC Services**" is the specific supply of services agreed under an Order.
"**Customer Data**" is the Personal Data provided by the Customer to BMC in accordance with an Agreement executed by the parties.
"**European Data Protection Laws**" means European Directive 95/46/EC and national data protection regulations applicable in the European Economic Area.
"**Order**" or "**SOW**" is an agreed written or electronic document, subject to the terms of the Agreement and this DPA, that identifies the BMC Products and/or BMC Services supplied from BMC to Customer and the fees to be paid by Customer to BMC.
"**Personal Data**", "**data processor**", "**data controller**", "**processing**" have the meaning specified for each term respectively under the European Data Protection Laws.
"**Sub-processor**" means any data processor engaged by BMC that processes Customer Data that may be an Affiliate of BMC or a third party engaged by BMC.

2. **SCOPE**. This DPA applies to the transfer and processing of data for the purpose of processing Customer Data in accordance with European Data Protection Laws upon execution of an Order that refers to this DPA. Capitalized terms not defined herein shall have the meanings given to them in the Order or in the Agreement. In the event of a direct conflict between the Agreement, any Order and the terms of this DPA, the terms of the Order will control only if the Order is agreed to by each party.

3. **TERM**. This DPA shall commence on 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 Customer Data by BMC is necessary for the purpose of the Order, the Agreement or as required by law (e.g. return of Customer Data), this DPA shall continue to apply until the completion of the purpose or return, as applicable.

4. **PROCESSING OF CUSTOMER DATA.**

4.1 **Roles of the Parties**. As between the parties, Customer as the data controller determines the purposes and means of processing of Customer Data. BMC, as the data processor, processes Customer Data on behalf of Customer.

4.2 **Purpose**. BMC shall process and use Customer Data for the purposes defined in Attachment 1 to this DPA and in accordance with the Customer's instructions as set forth in the Agreement, the Order and this DPA. Customer hereby instructs BMC to process Customer Data necessary for the exercise and performance of Customer's rights and obligations under the Agreement, the Order and this DPA. Customer Data may be processed or used for another purpose only with the prior written consent of Customer. The Customer maintains all rights in Customer Data and in all copies thereof.

4.3 **Instructions**. Customer's instructions to BMC for the processing of Customer Data shall comply with European Data Protection Laws, this DPA and the Agreement. Instructions are to be provided in writing.

4.4 **Information**. 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 Customer Data, then to the extent the Customer does not have access to that information in its use of the BMC Products and/or BMC Services, 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.

5. **SUB-PROCESSING**. Customer acknowledges and agrees that BMC may engage its Affiliates or third parties as Sub-processors to assist in the provision of BMC Products and BMC Services only, including access to Customer Data. A list of all Sub-procesors (including BMC Affiliates and third party Sub-processor) as of the Effective Date of this DPA is provided in Attachment 2 to this DPA. Any additions, removals or amendments to this list will be notified to Customer via email. Sub-processors of Customer 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 the least the same level of privacy protection as is required by this DPA and the Agreement. This DPA does not govern the processing of data by third parties not engaged by BMC or the usage by Customer of third party applications that are not part of the BMC Products and/or BMC Services. BMC is responsible for the acts and omissions of its Sub-processors to the same extent BMC would be liable if performing the supply of BMC Products and/or BMC Services of each Sub-processor directly under the terms of this DPA.

6. **TRANSFER OF CUSTOMER DATA TO THIRD COUNTRIES**. If transfer of Customer Data outside of the EEA (or other countries with adequate level of protection as per the European Data Protection Laws) is required, BMC will transfer such Customer Data pursuant to the BCRs as approved by European data protection authorities. The BCR policy is incorporated into a BMC corporate wide policy, requiring all BMC Affiliates and their employees to comply with and respect the BCR policy which is governing the collection, use, access,

storage and transfer of Customer Data among BMC Affiliates and third party Sub-Processors. Customer agrees to rely upon the BCR as providing adequate safeguards in regard to European 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. Customer agrees that Customer Data may be processed by BMC Affiliates and third party Sub-Processors provided that BMC, its Affiliates and its Sub-Processors are and remain contractually bound by the BCR, or in the case of Sub-Processors by the Sub-Processor's own BCR. BMC represents that its Affiliates and Sub-Processors are and shall for the duration of this DPA remain contractually bound by and comply with the requirements of the BCR, or in the case of Sub-Processors by the Sub-Processor's own BCR.

7. **DELETION AND RETURN.** To the extent Customer cannot correct, delete or block Customer Data in its use of the BMC Products and/or BMC Services, BMC shall assist Customer within a reasonable period of time. Upon request by Customer made within thirty (30) days after the effective date of termination of the Order(s), BMC will at its discretion either delete or return all the Customer Data to the Customer. After such 30-day period, if BMC has not already done so, BMC will delete the Customer Data from the BMC Services, including copies, unless legally prohibited.

8. **SECURITY**.

8.1 **Confidentiality**. BMC shall treat Customer Data as Confidential Information and shall comply with European Data Protection Laws applicable to BMC as a data processor in providing the BMC Products and BMC Services. BMC shall ensure that all personnel of BMC granted access to Customer Data have executed written confidentiality obligations with a level of protection as required under the Agreement. The obligation to treat Customer Data pursuant to such confidentiality obligations shall survive the termination of the employment, and only so long as such Customer Data is considered Confidential Information. Customer Data may be made available only to personnel that require access to such Customer Data for the performance of this DPA.

8.2 **Organizational and technical protection measures**. BMC shall implement appropriate organizational and technical protection measures, as set out in Attachment 3 to this DPA. BMC regularly monitors compliance with these measures. Notwithstanding the aforementioned, 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.

8.3 **Appointment of a Data Protection Officer**. BMC, BMC Affiliates and Sub-processors have appointed a data protection officer where such appointment is required by applicable law. Upon request, BMC will provide the contact details of such appointed persons.

9. **MANAGEMENT**. If BMC receives any complaint, notice, or communication that relates to BMC's processing of Customer Data in connection with an Order, 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. Additionally, BMC shall promptly inform Customer about any of the following: (i) infringements of European Data Protection Laws that relate to Customer Data processed by BMC; (ii) actual or reasonably suspected unauthorized access to or disclosure of Customer Data of which BMC becomes aware. Any BMC obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this DPA.

10. **LIMITATION OF LIABILITY.** Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement.

ATTACHMENTS INCORPORATED INTO THIS DPA	
Attachment 1 – Details of Customer Data processing	X
Attachment 2 – List of Sub-processors	X
Attachment 3 – Organizational and technical protection measures	X

Attachment 1 - Details of Customer Data processing

1. Extent, Type and Purpose of intended processing or Use of Data

As set forth in the Agreement, BMC shall process the Customer Data necessary for the exercise and performance of Customer's rights and obligations under the Agreement, the Order and this DPA.

Additionally, as set forth in the DPA, BMC shall not disclose Customer Data except as expressly permitted in writing by Customer or where required by law, in which case, to the extent legally permitted, BMC will provide Customer with prior notice of any such compelled disclosure.

2. Categories of Customer Data and concerned Data Subjects

(a) Data Subjects

The Customer Data concern the following categories of Data Subjects:

- Customers
- Prospective Customers
- Employees
- Suppliers

(b) Categories of Data

The Customer Data concern he following categories of data:

- 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

Attachment 2 - List of Sub-processors

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 Party entities for BMC Support		
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
Additional third party entities may be called out on Orders		

Attachment 3 - Organizational and technical protection measures

A. GENERAL ORGANIZATIONAL AND TECHNICAL MEASURES

As part of the applicable Order, BMC is supplying Customer with BMC Products and/or BMC Services to Products installed on the Customer's environments and therefore BMC does not generally process Customer Data. To the extent Customer elects to provide Customer Data to BMC in accordance with the relevant Order, the Agreement and this DPA, the following oganizational and protection measures apply.

1. **Access control to premises, facilities and assets to prevent unauthorized persons from gaining access to data processing systems for processing or using Customer 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.
   - Accounts and access are revoked immediately upon termination of employment of such BMC user account, including disconnection of active remote access sessions.
   - BMC User Accounts are generated on a per-individual basis and not shared.
   - For BMC Support, access to MFT service is restricted to authorized personnel only, which is limited to BMC Support and the customer.
   - For BMC Support, BMC's MFT service is deployed in physically redundant, geographically diverse locations.
   - For BMC Professional Services, access to BMC endpoints is restricted to authorized personnel only which is limited to BMC Support Services and BMC Professional Services organizations.
   - BMC's data centers are with Tier 4 providers, with:
     - Multiple certifications including: SSAE 16 (SOC I type II), PCI DSS (sec 9 & 12), HIPAA, ISO 27001, FISMA
     - 24 hour security
     - Restricted, multifactor access
   - BMC systems within the data center are:
     - Located in a private space, accessible by BMC authorized personnel only
     - Operated on hardware owned by BMC
     - Operated on a BMC private network, accessible by BMC authorized personnel and assets only

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:

   - BMC user accounts are required in order to access BMC systems. Access is restricted to BMC Support personnel, and the assigned system owner.

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 Customer Data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.**

   - BMC maintains a confidential information protection policy that outlines data handling practices based on classification for which all BMC employees must comply.
   - BMC user accounts are required to access BMC systems, and are restricted to authorized BMC Support personnel and assigned system owner.

B. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO SUPPORT

1. **Disclosure control to ensure that Customer 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 Customer Data are to be transferred by means of data transmission facilities.

- BMC has deployed security measures to ensure that Customer Data is fully encrypted, using AES 256, in transport as it moves from the Customer site to Support MFT system.
- Customer communication to the MFT system requires the use of an encrypted transmission channel using Secure File Transfer Protocol (SFTP).
- BMC utilizes AES-256 encryption on disk, to ensure that data at rest on the MFT system cannot be read without authorization.

2. **Input control to ensure that it is possible to after-the-fact check and establish whether Customer 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 MFT systems where the Customer Data potentially resides.
- Logging provides full accountability for actions taken against Customer Data. Logs are retained for a period of at least a consecutive twelve (12) months.

3. **Job control to ensure that Customer Data processed on behalf of others are processed strictly in compliance with the data controller's instructions.**

- BMC does not process Customer Data. In the event Customer provides Customer Data for support purposes, the support MFT system provides automatic scanning of the stored data to attempt to detect any sensitive data.
- If sensitive data is detected, both the Customer and BMC support personnel are alerted so special handling procedures can be taken if needed.

4. **Availability control to ensure that Customer 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 our 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.

C. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO SUBSCRIPTION SERVICES

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

In data centers, the following measures are deployed to protect and control secured access to data center facilities:

- Access to production and disaster recovery data centers is securely controlled and monitored by industry standard layers of security.
- No entry to data center sites without approved change control, photo ID card and security center clearance.

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

The following controls are implemented:

- Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
- User passwords are stored using a one-way hashing algorithm and are never transmitted unencrypted.
- Access to the Services require a valid User ID and password combination, which are encrypted via current industry encryption standards while in transmission. Following a successful authentication, a random session ID is generated and stored in the User's browser to preserve and track session state.
- Controls to ensure generated initial passwords must be reset on first use.
- Controls to revoke access after several consecutive failed login attempts.
- Controls on the number of invalid login requests before locking out a User.

- Controls to force a User password to expire after a period of use.
- Controls to terminate a User session after a period of inactivity.
- Password history controls to limit password reuse.
- Password length controls
- Password complexity requirement.
- Verification question before resetting password.

3. **Access control to data to ensure that persons authorized 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.**

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.**

   Security measures are employed to ensure that Personal Data is fully encrypted during transmission between Customer's network and the XaaS services data centers.

   Customer communication to any XaaS services data center requires the use of an encrypted transmission channel, including at least HyperText Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS). Additional encrypted transmission channels may also include but are not limited to, Secure File Transfer Protocol (SFTP) and 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.**

   Controlled and secured logging procedures may be employed by Customer on XaaS services systems where the Personal Data resides. Logging provides full accountability for actions taken against Personal Data and by whom within the XaaS Services organization.

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 and its Subcontractor shall process Personal Data in accordance with Customer's lawful and explicit instructions, including to provide the Services as set forth in the Agreement and as instructed by Users in their use of the Services.

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

   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.

   - Disaster recovery. BMC or its Subcontractor may utilize disaster recovery facilities that may be geographically remote from primary data centers, along with required hardware, software, and Internet connectivity, in the event BMC's Subcontractor production facilities at the primary data center were to be rendered unavailable. BMC's Subcontractor has disaster recovery plans in place and tests them at least once per year.
   - Viruses. The Services will not introduce any viruses to Customers systems; however, the Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Services.

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

   - Permissions and access control lists within BMC Subscription Services environment allow logically segregated processing of personal data;
   - Access control within the BMC Subscription Services environment is restricted and isolated so usage activities for one BMC customer cannot be viewed or accessed by another BMC customer.

D. ORGANIZATIONAL AND TECHNICAL MEASURES APPLYING ONLY TO CONSULTING SERVICES

1. **Disclosure control to ensure that Customer 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.**

   - BMC has deployed security measures to ensure that BMC Professional Services computing systems (the PS laptops) are fully encrypted, using AES 256.
   - BMC Professional Services consultants utilize secure transmission methods for data transfer to/ from customer, such as SFTP.

2. **Availability control to ensure that Customer 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 our 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.