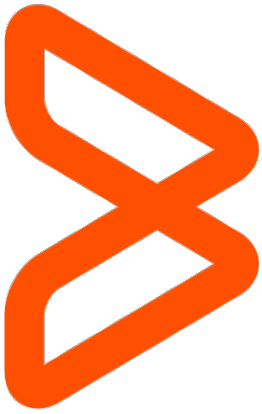

UK Processor Data Protection Binding Corporate Rules of BMC Software

bmc

Article I. TABLE OF CONTENTS

Article I. TABLE OF CONTENTS 1

Article II. INTRODUCTION 2

PART I: BACKGROUND AND ACTIONS 3

WHAT IS UK DATA PROTECTION LAW? 3

HOW DOES UK DATA PROTECTION LAW AFFECT BMC INTERNATIONALLY? 3

WHAT IS BMC DOING ABOUT IT? 3

FURTHER INFORMATION 4

PART II: BMC COMMITMENTS AS A PROCESSOR 5

SECTION A: BASIC PRINCIPLES 6

SECTION B: PRACTICAL COMMITMENTS 11

SECTION C: THIRD PARTY BENEFICIARY RIGHTS 14

PART III: APPENDICES 17

APPENDIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE 17

APPENDIX 2 - COMPLIANCE STRUCTURE 22

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS 25

APPENDIX 4 - AUDIT PROTOCOL 28

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE 31

APPENDIX 6 - COOPERATION PROCEDURE 33

APPENDIX 7 - UPDATING PROCEDURE 34

APPENDIX 8 - MATERIAL SCOPE OF THE PROCESSOR POLICY 38

APPENDIX 9 - LIST OF BCR GROUP MEMBERS 49

APPENDIX 10 - LIST OF DEFINITIONS 59

Article III. PART IV: DOCUMENT INFORMATION 60

Article II. INTRODUCTION

These UK[1] Processor Data Protection Binding Corporate Rules of BMC Software (the "**Processor Policy**") establish BMC Software's approach to compliance with UK Data Protection Law when transferring Personal Information between the BMC group members ("**Group Members**" or "**BMC**"), listed in Part III, Appendix 9.

The Processor Policy describes the standards that Group Members must apply when they transfer Personal Information which is subject to transfer restrictions under the UK GDPR.

Personal Information subject to UK GDPR may be (i) transferred out of the UK by Group Members then processed by Group Members outside of the UK, on behalf of a controller, or (ii) transferred from Group Members outside the UK in accordance with the scope described in Article 3 of UK GDPR. In the event such Personal Information is transferred to countries considered as adequate in accordance with UK GDPR, this Processor Policy shall be the preferred transfer instrument, rather than relying on the adequacy mechanism.

In this context, BMC may transfer Personal Information listed in Appendix 8. Such Personal Information may be transferred to all countries where BMC entities listed in Appendix 9 as UK BCR Group Members are located. For additional details about the material scope of the Processor Policy and the list of BCR Group Members, you may refer to Appendices 8 and 9.

Transfers of Personal Information take place between Group Members during the normal course of business and such information may be stored in centralized databases accessible by Group Members from anywhere in the world.

The Processor Policy does not replace any specific data protection requirements under UK Applicable Law that might apply to a business area or function.

The Processor Policy will be published in full on the BMC website accessible at www.bmc.com and on the BMC intranet.

[1] United Kingdom

PART I: BACKGROUND AND ACTIONS

WHAT IS UK DATA PROTECTION LAW?

UK Data Protection law gives people certain rights in connection with the way in which their "**Personal Information**"[2] is processed[3]. If organizations do not comply with data protection law, they may be subject to sanctions and penalties imposed by the UK Information Commission (the "**Commission**") and UK courts. Under UK data protection law, when an organization collects, processes or transfers Personal Information for its own purposes, that organization is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the legal requirements. When, on the other hand, an organization processes Personal Information on behalf of a third party (for example, to provide a service), that organization is deemed to be a *processor* of the information and the third party will be primarily responsible for meeting the legal requirements as a controller. The Processor Policy describes how BMC will comply with data protection law in respect of processing undertaken in its capacity **as a processor**. BMC also acts as a controller and has set out its commitments in its UK Controller Data Protection Binding Corporate Rules of BMC Software (the "**Controller Policy**").

HOW DOES UK DATA PROTECTION LAW AFFECT BMC INTERNATIONALLY?

UK Data Protection Law prohibits the transfer of Personal Information to countries outside the UK that do not ensure an adequate level of data protection. Some of the countries in which BMC operates are not regarded by UK Data Protection Law as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS BMC DOING ABOUT IT?

BMC must take proper steps to ensure that it processes Personal Information on an international basis in a safe and lawful manner. The purpose of the Processor Policy, therefore, is to set out a framework to satisfy the standards contained in UK Data Protection Law and, as a result, provide an adequate level of protection for all Personal Information processed and collected in the UK or otherwise protected by UK Data Protection Law and transferred to Group Members.

---

[2] "Personal Information" means any information relating to an identified or identifiable living individual, in line with the definition of "personal data" in the UK Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK GDPR**") as incorporated into and amended by the European Union (Withdrawal) Act 2018 as amended or superseded from time to time (together, "**UK Data Protection Law**").

[3] "Processing" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

BMC will apply the Processor Policy globally, and in **all cases** where BMC processes Personal Information both manually and by automatic means when the Personal Information relates to our Clients:

- prospects, customers, business partners and vendors;
- personnel, including employees, agents and contractors; and
- users authorized by customer to use BMC Services.

Additional details about the material scope of the Processor policy are set out in Appendix 8**.**

The Processor Policy applies to all Group Members and their employees worldwide, and requires that Group Members who collect, processed or transfer Personal Information to provide services to a third party as a processor or who provide a service to other Group Members in their capacity as a processor must comply with **Part II** of the Processor Policy together with the practical procedures set out in the appendices in **Part III** of the Processor Policy.

This Processor Policy is made binding on all Group Members via an Intra-Group Agreement and applies to all the employees of the Group Members either via their employment agreement and/or directly via BMC's corporate policies which relate to this matter and which carry disciplinary actions in case of violation of such policies, including this Processor Policy, up to and including termination of employment. As for contractors and/or contingent workers, this Processor Policy is expressly referred to in their service agreement and violation of this Processor Policy can lead to termination of such service agreement.

FURTHER INFORMATION

If you have any questions regarding the provisions of the Processor Policy, your rights under the Processor Policy or any other data protection issues, you can contact BMC's Group Data Protection Officer at the address below who will either deal with the matter or forward it to the appropriate person or department within BMC.

Maxime Roze

Group Data Protection Officer

Phone: +33 (0)1.57.00.62.60

Email: privacy@bmc.com

Address: Cœur Défense - Tour A, 10ème étage, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, FRANCE

The Group Data Protection Officer is responsible for monitoring compliance with the Processor Policy and ensuring that changes to the Processor Policy are notified, to the Group Members, to Clients (defined below), to the Commission and to individuals whose Personal Information is processed by BMC, as required by UK Applicable Law. If you are unhappy about the way in which BMC has processed your Personal Information, BMC has a separate complaint handling procedure which is set out in Part III, Appendix 5.

PART II: BMC COMMITMENTS AS A PROCESSOR

The Processor Policy applies in all cases where BMC collects, processes and transfers Personal Information **as a processor** on behalf of a third party under a contract evidenced in writing in a situation where the third party will be a controller (referred to as the "**Client**" or the "**Controller**" in this Processor Policy).

The principal areas in which BMC acts as a processor include the provision of software as a service. Additional details about the material scope of the Processor policy are set out in Appendix 8**.**

When BMC acts as a processor, the Client retains the responsibility to comply with UK Data Protection Law as a controller. Certain data protection obligations are passed to BMC in the contracts BMC has with its Clients, in accordance with UK Applicable Law. If BMC fails to comply with such data protection obligations, BMC may face a civil claim for breach of contract which may result in the payment of compensation or other judicial remedies, as well as an administrative sanction for a breach of applicable data protection law. If a Client demonstrates that it has suffered damage, and that it is likely that the damage occurred because of a breach of the Processor Policy (as applicable) by a Group Member outside the UK or by a third party sub-processor established outside the UK, that Client is entitled to enforce this Processor Policy against BMC Software Ltd ("**UK Group Member**"). In such cases, the obligation will be on the UK Group Member to show that a Group Member outside the UK (or a third party sub-processor established outside the UK) is not responsible for the breach, or that no such breach took place.

Although it will be for each of BMC's Clients to decide whether the commitments made by BMC in the Processor Policy provide adequate safeguards for the Personal Information transferred to BMC under the terms of its contract with BMC, BMC will apply the Processor Policy whenever it acts as a processor for a Client. Where BMC's Clients rely upon the Processor Policy as providing adequate safeguards, the Processor Policy will be incorporated into the contract with that Client by reference. If a Client of BMC chooses not to rely upon the Processor Policy, that Client will have the responsibility to put in place other adequate safeguards to protect the Personal Information.

It is up to the Client to decide whether this Processor Policy shall apply to:

i) Personal information subject to UK Applicable Law; or

ii) All Personal Information whatever the origin of the Personal Information.

Part II of the Processor Policy is divided into three sections:

- **Section A**: addresses the basic principles that BMC must observe when BMC collects and processes Personal Information as a processor.
- **Section B**: deals with the practical commitments made by BMC to the Commission when BMC collects and processes Personal Information.
- **Section C**: describes the third party beneficiary rights that BMC has granted to individuals in its capacity as a processor under Part II of the Processor Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH THIRD COUNTRY NATIONAL LEGISLATION AND ACCOUNTABILITY

Rule 1A – BMC will comply with the Processor Policy except if applicable third country national legislation requires a higher level of protection for Personal Information

To the extent that any applicable third country national legislation requires a higher level of protection for Personal Information, BMC acknowledges that such legislation will take precedence over the Processor Policy.

Where such third country national legislation does not exist or where it provides a lower level of protection, the protection provided by the Processor Policy shall not be undermined.

Where BMC believes that applicable third country national legislation prevents it from fulfilling the instructions received from the Controller or its obligations under the Processor Policy, Rule 12A shall apply.

Rule 1B – BMC will cooperate and assist its Clients to comply with its obligations under data protection law in a reasonable time and to the extent reasonably possible.

BMC will, within a reasonable time, to the extent reasonably possible and according to the terms agreed in its contracts with its Clients, assist its Clients to comply with their obligations as controllers under applicable data protection law. This may include, for example, cooperating and assisting its Clients to respect the individuals' rights or to handle their complaints, or being in a position to reply to investigation or inquiry from the Commission.

Pursuant to Articles 25 and 47.2 (d) of UK GDPR, all Group Members shall also assist the Controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by this Policy in practice, such as data protection by design and by default.

Rule 1C – BMC will make available to its Clients all information necessary to demonstrate compliance with BMC's obligations under the Processor Policy.

In accordance with Articles 28.3 (h), 30 and 47.2 d) of UK GDPR, BMC will maintain a written record (including in electronic form) of the processing activities carried out by all Group Members on behalf of its Clients, in line with the requirements set out in UK Data Protection Law and which may be made available to the Commission upon request. BMC will make available to its Clients all information necessary to demonstrate compliance with its obligations under UK Data Protection Law, and will allow for and contribute to audits, including inspections conducted by the Client.

Rule 1D – BMC will make the Processor Policy binding through a Service Agreement with its Clients

BMC will enter into a Service Agreement with its Clients, making the Processor Policy binding through a specific reference to the Policy. The BCR Policy will be made available or appended in full. The Service Agreement will make a specific reference to this Policy, which shall be annexed to the Service Agreement or

a reference to it will be made with electronic access. The Service Agreement will comply with Article 28 of UK GDPR.

RULE 2 – ENSURING TRANSPARENCY, FAIRNESS, LAWFULNESS AND PURPOSE LIMITATION

Rule 2A – BMC will assist its Clients in ensuring transparency, fairness and lawfulness.

Clients have a duty to explain to individuals, at the time their Personal Information is collected or shortly after, how that information will be processed and this is usually done by means of an easily accessible fair processing statement. In addition, Clients must ensure that Personal Information is processed lawfully and fairly.

BMC will assist its Clients in complying with such requirements as per the terms of its contracts with its Clients and Group Members.

Rule 2B – BMC and its sub-processors will only process Personal Information on behalf of and in accordance with the specific instructions of its Clients ("Purpose limitation").

BMC and its sub-processors, including their employees, will only process Personal Information in compliance with the terms of a contract it has with its Client, including when it relates to transfers of Personal Information to a third country in accordance with Article 28.3(a) of UK GDPR, unless otherwise required by UK Applicable Law.

In such a case, BMC shall inform the Client of that legal requirement before processing takes place, unless that law prohibits such information from being disclosed on important grounds of public interest.

BMC shall immediately inform its Clients if in its opinion, an instruction infringes UK Data Protection Law.

If, for any reason, BMC and its sub-processors are unable to comply with this Rule or its obligations under the Processor Policy in respect of any contract it may have with a Client, BMC will inform that Client promptly of this fact. BMC's Client may then suspend the transfer of Personal Information to BMC and/or terminate the contract, depending upon the terms of its contract with BMC.

On the termination of the provision of services to a Client, BMC and its sub-processors will, at the choice of the Client, delete or return all Personal Information to the Client and delete the copies thereof, as required in accordance with the terms of its contract with that Client, unless UK Applicable Law requires storage of Personal Information by BMC. In that case, BMC and its sub-processors will maintain the confidentiality of the Personal Information and will no longer actively process that Personal Information for the purposes for which it was initially collected, but only to comply with UK Applicable Law.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3 – BMC and its sub-processors will assist its Clients to keep the Personal Information accurate and up to date.

BMC will comply with any instructions from a Client under the terms of its contract with that Client, in order

to assist them to comply with their obligation to keep Personal Information accurate and up to date.

When required to do so on instruction from a Client, as required under the terms of its contract with that Client, BMC and its sub-processors to whom Personal Information has been provided, will delete, anonymise, update, correct Personal Information, or cease or restrict from processing Personal Information.

BMC will promptly notify other Group Members or any third party sub-processor to whom the Personal Information has been disclosed accordingly so that they can also update their records.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – BMC and its sub-processors will assist Clients to comply with the rights of individuals.

In accordance with Article 12.3 and 28.3 (e) of UK GDPR, BMC and its sub-processors will act in accordance with the instructions of a Client as required under the terms of its contract with that Client and undertake any appropriate technical and organizational measures to enable its Clients to comply with their duty to respect the rights of individuals. In particular, if BMC receives an individual's rights request, it will transfer such request promptly to the relevant Client and not respond to such a request unless authorized to do so or required by UK Applicable Law. Such assistance shall be provided as set out in Chapter III of UK GDPR (Art. 28.3 (e) of UK GDPR) including by communicating any useful information in order to help the Controller to comply with the duty to respect the rights of the individuals.

The full request handling procedure is further described in Appendix 1 Part III of this Processor Policy.

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – BMC and its sub-processors will put in place appropriate technical and organizational measures to safeguard Personal Information processed on behalf of its Clients to ensure a level of security appropriate to the risk.

In accordance with Article 28.3 (f) and 32 of UK GDPR, where BMC provides a service to a Client which involves the processing of Personal Information, the contract between BMC and its Client details the security and organizational measures required to safeguard that information in a manner appropriate with the associated level of risk and consistent with UK Applicable Law. BMC and its sub-processors shall implement such security and organizational measures and respect the instructions from the Controller regarding the processing of Personal Information, including the security and confidentiality measures. Pursuant to Article 28.3 (f) of UK GDPR, BMC and its sub-processors will assist the Client in ensuring compliance with Article 32 to 36 of UK GDPR, considering the nature of processing and information available to BMC.

Rule 5B – BMC will notify its Clients of any Personal Information breach in accordance with the terms of the contract with the Client.

In accordance with Article 33.2 of UK GDPR, BMC will notify a Client of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information breach in relation to Personal Information processed on behalf of that Client without undue delay and as required to do so under the terms

of the contract with that Client. Furthermore, any Personal Information breach shall be documented (including the facts relating to the breach, its consequences and any remedial action taken). Such documentation will be made available to the Commission in accordance with the UK GDPR.

Rule 5C – BMC will comply with the requirements of its Clients regarding the appointment of any sub-processor.

Rule 5C a) – Appointment of a Group Member as a sub-processor

In accordance with Articles 28.2, 28.3 (d), 28.4, 45, 46 and 47 of UK GDPR, BMC will inform its Clients where processing undertaken on their behalf will be conducted by a Group Member, and will comply with the particular requirements of a Client with regard to the appointment of sub-processors as set out under the terms of its contract with that Client. BMC will ensure that up to date information regarding its appointment of sub-processors is available to those Clients at all times. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or a specific authorization will be required for each new sub-processor. If a general authorization is given, the Client should be informed by BMC of any intended changes concerning the addition or replacement of a sub-processor in such a timely fashion that the Client has the possibility to object to the change or to terminate the contract before the Personal Information are communicated to the new sub-processor.

Rule 5C b) – Appointment of an external service provider as a sub-processor

In accordance with Articles 28.2, 28.3 (d), 28.4, 45, 46 and 47 of UK GDPR, BMC will inform its Clients where processing undertaken on their behalf will be conducted by an external service provider, and will comply with the particular requirements of a Client with regard to the appointment of sub-processors as set out under the terms of its contract with that Client. BMC will ensure that up to date information regarding its appointment of sub-processors is available to those Clients at all times. The Service Agreement Client will specify if a general prior authorization given at the beginning of the service would be sufficient or a specific authorization will be required for each new sub-processor. If a general authorization is given, the Client should be informed by BMC of any intended changes concerning the addition or replacement of a sub-processor in such a timely fashion that the Client has the possibility to object to the change or to terminate the contract before the Personal Information are communicated to the new sub-processor.

Rule 5D – BMC will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms of its contracts with its Clients and (ii) the Processor Policy, and in particular that the sub-processor will adopt appropriate and equivalent technical and organizational measures.

BMC must only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by BMC in Part II of the Processor Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their processing of the Personal Information to which they will have access in accordance with the terms of the contract between BMC and a

Client and Article 28.3 c) of UK GDPR.

To comply with this Rule, BMC will take steps to ensure that it has in place appropriate technical and organizational security measures to safeguard the Personal Information in accordance with Article 32 of UK GDPR and will impose strict contractual obligations in writing on the sub-processor which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in Part II of the Processor Policy (and in particular Rules 5A and 5B above) and with the terms of the contract BMC has with a Client in respect of the processing in question;
- that the sub-processor will act only on BMC's instructions when processing that information;
- that the sub-processor will cooperate with the Commission and the Client in a similar way as BMC as detailed in part II of the Processor Policy; and
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by BMC in Part II of the Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of Personal Information from a Group Member to a sub-processor

Contracts with sub-processors shall provide adequate protection as set out in Articles 28, 29, 32, 45, 46, 47 of UK GDPR and shall ensure that the same data protection obligations (as set out in the Service Agreement between BMC and its Clients) are imposed on the sub-processors.

Such contracts shall include all rights and obligations as further described in the Processor Policy. They shall include in particular:

- a requirement to process Personal Information solely on instructions communicated by BMC, which shall include Client's instructions. BMC's instructions shall not conflict with or undermine Client's instructions;
- the rights and obligations of the Client;
- the scope of processing (duration, nature, purpose and the categories of Personal Information);
- an obligation for the sub-processor to:
  - implement appropriate technical and organizational measures to protect the Personal Information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access;
  - provide full cooperation and assistance to BMC to enable BMC to comply with its obligations under Rules 5A and 5B;
  - provide full cooperation and assistance to Client to allow individuals to exercise their rights under the Processor Policy;
  - provide full cooperation to Client so they can demonstrate its compliance obligations – this includes the right of audit and inspection;
  - make all reasonable efforts to maintain the Personal Information so that they are accurate and up to date at all times;
  - return or delete the data at our request or the request of a Client, unless required to retain some or part

of the data to meet other legal obligations; and

- maintain adequate confidentiality arrangements and not disclose the Personal Information to any person except as required or permitted by law or by any agreement between the Client and BMC or with the Client's written consent.

SECTION B: PRACTICAL COMMITMENTS

RULE 6 – COMPLIANCE

Rule 6 – BMC will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

BMC has appointed a Group Data Protection Officer who is part of the Core Privacy Team to oversee and ensure compliance with the Processor Policy. The Core Privacy Team is supported by legal and compliance officers at regional and country level who are responsible for overseeing and enabling compliance with the Processor Policy on a day-to-day basis. A summary of the roles and responsibilities of BMC's privacy team is set out in Appendix 2.

RULE 7 – TRAINING

Rule 7 – BMC will provide appropriate training to employees who have permanent or regular access to Personal Information, who are involved in the collection of Personal Information or in the development of tools used to process Personal Information in accordance with the Privacy Training Requirements set out in Appendix 3.

RULE 8 – AUDIT

Rule 8 – BMC will comply with the Processor Data Protection Binding Corporate Rules Audit Protocol set out in Appendix 4.

RULE 9 – COMPLAINTS

Rule 9 – BMC will comply with the Processor Data Protection Binding Corporate Rules Complaint Handling Procedure set out in Appendix 5.

RULE 10 – COOPERATION WITH THE COMMISSION

Rule 10 – BMC will comply with the Processor Data Protection Binding Corporate Rules Cooperation Procedure set out in Appendix 6.

RULE 11 – UPDATES TO PART II OF THE PROCESSOR POLICY

Rule 11 – BMC will comply with the Processor Data Protection Binding Corporate Rules Updating Procedure set out in Appendix 7.

RULE 12 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 12A – BMC will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under the Processor Policy or such legislation has a substantial effect on its ability to comply with the Processor Policy.

1. Assessment

BMC must assess, in light of all of the circumstances of a transfer, if the laws and practices in a third country, applicable to the processing of the Personal Information under this Policy, may impinge on the effectiveness of this Policy and thus prevent BMC from fulfilling its obligations under this Policy or has a substantial effect on the guarantees provided by this Policy.

In case where such third country has not been recognized by the UK as ensuring an adequate level of protection, BMC will carry out and document a transfer risk assessment, and make it available to the Commission on request.

For the avoidance of doubt, this section also pertains to further transfers of Personal Information to controllers and processors that are not Group Members.

2. Notification

If BMC has reason to believe that it is or has become subject to laws or practices not in line with the requirements under this Policy, including following a change in the laws of third countries or a measure indicating an application of such laws in practice that is not in line with the requirements of this Policy, BMC will promptly inform:

(a) the controller, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority);

(b) BMC's Group Data Protection Officer; and

(c) The Commission;

except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

3. Supplementary measures

Following a notification pursuant to section 2, or if BMC otherwise has reason to believe that it can no longer fulfil its obligations under this Policy, the controller shall promptly identify supplemental measures (such as technical or organizational measures to ensure security and confidentiality) to be adopted by BMC to address the situation.

BMC shall suspend the transfer of Personal Information if it considers that no appropriate measures for such transfer can be ensured, or if instructed by the controller or the Commission, including, to do so. In this case, the controller shall be entitled to suspend the transfer of Personal Information to BMC and/or terminate the contract, depending upon the terms of its contract with BMC.

Rule 12B – BMC will take appropriate action if (i) it receives a legally binding request for the disclosure of Personal Information transferred pursuant to this Policy from a public authority of a third country (e.g. a law enforcement authority or state security body), including judicial authorities, under the laws

of a third country ("Request for Disclosure") or (ii) becomes aware of any direct access by public authorities to Personal Information transferred pursuant to this Policy in accordance with the laws of a third country

1. Notification

If BMC receives a Request for Disclosure or becomes aware of a direct access to Personal Information by a public authority in a third country, BMC will promptly notify:

(a) the controller, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority);

(b) BMC's Group Data Protection Officer; and

(c) where possible, the individual (if necessary, with the help of the controller).

Such notification shall include information about the Personal Information requested, the requesting authority, the legal basis for the Request and the response provided, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

BMC will put the Request on hold and inform the Commission, unless prohibited from doing so by a law enforcement authority or agency

If BMC is prohibited from notifying the controller and/or the individuals concerned, and/or prohibited from informing the Commission, under the laws of the third country, BMC will use its best efforts to obtain a waiver of the prohibition. BMC will document its best efforts in order to be able to demonstrate them on request of the controller.

If, despite having used its best efforts, BMC is not in a position to obtain a waiver of the prohibition, BMC will annually provide general information on the Requests it received to the Commission (e.g., number of applications for disclosure, type of data requested, requester if possible, etc.).

BMC will preserve the information pursuant to this section 1 for the duration of the service agreement with the controller and make it available to the Commission on request.

In no event shall BMC transfer Personal Information to any public authority in a third country in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

2. Review of legality and minimisation

BMC will review the legality of the Request for Disclosure and will challenge it if, after careful assessment, it concludes that there are reasonable grounds to consider that the Request for Disclosure is unlawful under the laws of third countries, applicable obligations under international law and principles of international comity.

BMC will, under the same conditions, pursue possibilities of appeal. When challenging a Request for Disclosure, BMC will seek interim measures with a view to suspending the effects of the Request until the competent judicial authority has decided on its merits. BMC shall not disclose the Personal Information requested until required to do so under the applicable procedural rules.

BMC will document its legal assessment and any challenge to the Request for Disclosure and, to the extent permissible under the laws of the third countries not recognized by the UK as ensuring an adequate level of protection, make the documentation available to the controller. BMC shall also make it available to the Commission on request, to the extent permissible under the laws of the third countries.

BMC will provide the minimum amount of information permissible when responding to a Request for Disclosure, based on a reasonable interpretation of the Request.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

UK Data Protection Law states that individuals meeting the criteria described in Article 3 of UK GDPR ("**UK Individuals**") must be given rights to enforce this Processor Policy as third party beneficiaries.

It is agreed that such third party beneficiary rights shall not be open to UK Individuals which Personal Information is not handled by BMC acting as a processor.

Third party beneficiary rights allow a UK Individual to enforce the following explicitly listed elements directly against BMC, acting as a processor:

- **duty to respect the instructions from the Controller regarding the Personal Information processing including for data transfers to third countries** pursuant to Articles 28.3 (a), 28.3 (g) and 29 of UK GDPR (Rule 2B, 5A, 5B and 5D Part II of this Processor Policy);
- **duty to implement appropriate technical and organizational security measures** pursuant to Articles 28.3 (c) and 32 of UK GDPR **and to notify any Personal Information breach to the controller** pursuant to Article 33.2 of UK GDPR (Rules 5A, 5B and 5D Part II of this Processor Policy);
- **duty to respect conditions when engaging a sub-processor either within or outside the Group Members** pursuant to Articles 28.2, 28.3(d), 28.4, 45, 46, 47 of UK GDPR (Rules 5C and 5D Part II of this Processor Policy);
- **duty to cooperate with and assist the Controller in complying and demonstrating compliance with UK Applicable Law, such as for answering requests from data subjects in relation to their rights** pursuant to Articles 28.3(e), (f) and (h) of UK GDPR (Rules 1B, 1C, 2A, 3, 4, and 5D Part II and Appendix 1 of this Processor Policy);
- **easy access to this Processor Policy** pursuant to Article 47.2(g) of UK GDPR (Section C (e) Part II of this Processor Policy);
- **right to complain through internal complaint mechanisms** pursuant to Article 47.2(i) of UK GDPR (Rule 9 Part II and Appendix 5 of this Processor Policy);
- **duty to cooperate with the Commission** pursuant to Articles 31 and 47.2(l) of UK GDPR (Rule 10 Part II of this Processor Policy and Appendix 6);

- **liability, compensation and jurisdiction provisions** pursuant to Articles 47.2(f), 79, 82 of UK GDPR (Section C Part II of this Processor Policy); and
- **national legislation preventing respect of this Processor Policy** pursuant to Article 47.2 (m) of UK GDPR (Rule 12 Part II of this Processor Policy).

A UK Individual may also enforce the above-mentioned rights against the UK Group Member if that UK Individual is not able to bring a claim against the Controller, because the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract of by operation of law, in which case the UK Individual can enforce its rights against such successor entity.

Should one of the enforceable elements listed above be breached, UK Individuals who benefit from third party beneficiary rights are entitled to seek the following actions:

(a) *Complaints to BMC:* UK Individuals may lodge a complaint to BMC in accordance with the Complaint Handling Procedure set out in Appendix 5 in accordance with Article 47.2 (i) of UK GDPR.

(b) *Complaints to the Commission*: UK Individuals may make a complaint to the Commission in accordance with Article 77 of UK GDPR.

(c) *Jurisdiction*: UK Individuals may bring proceedings against the UK Group Member before the UK courts in accordance with Article 79 of UK GDPR.

(d) *Liability*: In accordance with Articles 47.2 (f), 79, and 82 of UK GDPR, the UK Group Member shall accept responsibility for and agree to take the necessary action to remedy and to pay compensation for any material or non-material damages resulting from a violation of the above elements of the Processor Policy in the limited cases mentioned above, should such violation be caused by:

(i) a BMC Group Member located outside the UK and acting as a processor or as a sub-processor; or

(ii) an external sub-processor located outside the UK.

The UK Group Member will accept liability as if the violation had taken place by him in the UK instead of the processor or the sub-processor established outside the UK. In such case, UK Courts or other competent authorities in the UK will have jurisdiction.

In accordance with Article 82.4 of UK GDPR, where BMC, acting as a processor, and the Client, involved in the same processing, are found to be responsible for any damage caused by such processing, the concerned UK Individual shall be entitled to receive compensation for the entire damage directly from the processor. The concerned UK Individual shall not be required to go through judicial processes or to sign settlement or non-disclosures agreements in order to seek redress or compensation.

The UK Group Member may not rely on a breach by a sub-processor (internal or external) established outside the UK in order to avoid its liabilities.

(e) *Transparency and Easy access to Processor Policy:* In accordance with Article 47.2 (g) of GDPR, all concerned UK Individuals benefiting from third party beneficiary rights shall be provided with the information on such third party beneficiary rights with regard to the processing of their Personal Information and on the means to exercise those rights via a publication of the Processor Policy on www.bmc.com in full. Additionally, the Processor Policy is referenced in all Service Agreements entered into between BMC and a Client.

(f) *Burden of proof*: Where a Group Member established outside the UK is acting as a processor or a sub-processor, or should or an external sub-processor established outside the UK be used, and in the event that a UK Individual suffers damage where that UK Individual can demonstrate that it is likely that the damage has occurred because of a breach of the rights detailed hereabove, the burden of proof to show that such Group Member or such external sub-processor is not responsible for the breach, or that no such breach took place, will rest with the UK Group Member. If the UK Group Member can prove that such Group Member or such external sub-processor is not responsible for the act, it may discharge itself from any responsibility.

PART III: APPENDICES

APPENDIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE

1. Introduction

1.1 When BMC collects, processes or transfers Personal Information on behalf and under the instructions of a third party, such as a Client, BMC is deemed to be a *processor* of that information. The third party Controller will be primarily responsible for meeting the legal requirements as a *controller*.

1.2 This Individuals' Rights Requests Procedure ("**Procedure**") explains how BMC deals with an individual's rights request relating to Personal Information collected, processed or transferred by BMC as a processor, if authorized by a Client to do so and by provided it falls into the categories stated in section 1.3 below ("**Request**").

1.3 Individuals subject to UK GDPR have the following rights, which will be dealt with in accordance with the terms of this Procedure:

- Right of Access;
- Right to Rectification;
- Right to Erasure;
- Right to Restrict Processing;
- Right to Data Portability;
- Right to Object;
- Rights in relation to automated decision making and profiling.

1.4 Where Personal Information processing is based on consent, individuals also have the right to withdraw their consent at any time, in accordance with Article 7 of UK GDPR.

2. General Process

2.1 When BMC acts as a processor for a Client, Requests shall be primarily directed to the Client. In such case, BMC must assist and cooperate with the Client to respond to such Requests.

2.2 If BMC receives a Request in its capacity as a processor for a Client, BMC must transfer such Request promptly to the relevant Client and not respond to the Request unless authorized by such Client to do so. In case the Client has factually disappeared, or no longer exists in law, BMC shall handle the request directly.

2.3 Requests can be made in writing, which can include email, or orally in which case BMC will document the request and provide a copy to the individual making the request before dealing with it. Requests do not have to be official or to mention data protection law.

2.4 Requests will be passed to the Group Data Protection Officer via privacy@bmc.com immediately upon receipt, indicating the date on which it was received together with any other information which may

assist the Group Data Protection Officer to deal with the Request.

2.5 The Group Data Protection Officer will make an initial assessment of the Request to decide whether it is valid and whether confirmation of identity, or any further information, is required.

2.6 Where BMC has reasonable doubts about the identity of an individual making the Request, BMC may ask that additional information necessary to confirm the identity of that individual be provided.

2.7 BMC must respond to Requests without undue delay and in any event in accordance with the UK GDPR and the timescales agreed in the contract with the Client pursuant to UK GDPR.

BMC must act in accordance with the instructions of its Client and undertake any reasonably necessary measures to enable the Client to comply with its duty to respond to Requests.

2.8 BMC shall inform each recipient to whom Personal Information has been disclosed of the rectification or erasure of Personal Information, or restriction of processing, unless it is impossible or disproportionate to do so.

3. Right of Access

3.1 Individuals are entitled to obtain:

(i) confirmation as to whether or not Personal Information relating to them are being processed and, where that is the case;

(ii) access to the Personal Information processed by BMC on behalf of the relevant Client and the following information;

- purposes of the processing;
- categories of Personal Information concerned;
- recipients or categories of recipients to whom the information is disclosed, in particular recipients located in a third country. If the third country is not recognized by the UK as ensuring an adequate level of protection, individuals shall have the right to be informed of the appropriate safeguards authorizing such transfers;
- envisaged period for which the Personal Information will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of Personal Information, or restriction of processing of Personal Information, or to object to such processing;
- right to lodge a complaint with the Commission;
- any available information as to the source of Personal Information which has not been collected from the individual; and
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful

information about the logic involved in any automatic processing as well as the significance and the envisaged consequences of such processing for the individual.

4. Right to Rectification

4.1 Individuals are entitled to obtain the rectification of inaccurate Personal Information concerning them without undue delay. Taking into account the purposes of the processing, individuals have the right to have incomplete Personal Information completed, including by means of a supplementary statement.

5. Right to Erasure ('Right to be Forgotten')

5.1 Individuals are entitled to obtain the erasure of Personal Information concerning them without undue delay, where one of the following applies:

(i) Personal Information is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

(ii) the individual has withdrawn consent on which the processing was based, and there is no other legal ground for the processing;

(iii) the individual has objected to the processing and there are no overriding legitimate grounds for the processing, or the individual has objected to the processing for direct marketing purposes;

(iv) Personal Information has been unlawfully processed;

(v) Personal Information must be erased for compliance with a legal obligation in UK Applicable Law to which the relevant Client is subject; or

(vi) Personal Information has been collected in relation to the offer of information society services to children.

5.2 The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation as provided by UK Applicable Laws and regulations;
- for the performance of a task carried out in the public interest or in the exercise of official authority as provided by UK Applicable Laws and regulations;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

6. Right to Restrict Processing

6.1 Individuals are entitled to obtain restriction of processing, where one of the following applies:

(i) the accuracy of Personal Information is contested by the individual concerned, for a period enabling the

relevant Client to verify its accuracy;

(ii) the processing is unlawful and the individual opposes the erasure of the Personal Information and requests the restriction of their processing instead;

(iii) the relevant Client no longer needs the Personal Information for the purpose of the processing, but it is required by the individual for the establishment, exercise or defence of legal claims; or

(iv) the individual has objected to processing pending the verification whether the legitimate grounds of the relevant Client override those of the individual.

6.2 Where processing has been restricted under paragraph 6.1, Personal Information shall, with the exception of storage, only be processed with the individual's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the UK.

6.3 An individual who has obtained restriction of processing pursuant to paragraph 6.1 shall be informed by BMC before the restriction of processing is lifted.

7. Right to Data Portability

7.1 Individuals are entitled to receive their Personal Information in a structured, commonly used and machine-readable format and to transfer it to another controller without hindrance where:

(i) Personal Information is processed based on consent or on a contract with the individual; and

(ii)the processing is carried out by automated means.

7.2 In exercising his or her right to data portability pursuant to paragraph 7.1, the individual shall have the right to have the Personal Information transmitted directly from BMC to another controller, where technically feasible.

7.3 The exercise of the right referred to in paragraph 7.1 shall be without prejudice to the individual's right to erasure. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in BMC.

The right referred to in paragraph 7.1 shall not adversely affect the rights and freedoms of other individuals.

8. Right to Object

8.1 Individuals are entitled to object, on particular grounds, to processing of their Personal Information, where Personal Information:

(i) is processed based on public interest or official authority vested in the relevant Client, or the relevant Client's legitimate interests, unless the relevant Client has a compelling legitimate ground for the processing which overrides the interests, rights and freedoms of the Individual or for the establishment, exercise or defence of legal claims; and

(ii)is processed for direct marketing purposes, which includes profiling related to such direct marketing.

8.2 BMC shall no longer process the Personal Information unless BMC demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims.

8.3 At the latest at the time of the first communication with the individual, the right referred to in paragraph 8.1 shall be explicitly brought to the attention of the individual and shall be presented clearly and separately from any other information.

8.4 In the context of the processing of information society services, the individual may exercise his or her right to object by automated means using technical specifications.

8.5 Where Personal Information is processed for scientific or historical research purposes or statistical purposes, the individual, on grounds relating to his or her particular situation, shall have the right to object to processing of Personal Information concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

9. Right in relation to automated decision-making and profiling

9.1 Individuals are entitled not to be subject to a decision based on automated processing, including profiling, which produces legal effects or similarly significantly affects them, unless the decision:

(i) is necessary for entering into, or performing a contract between the relevant Client and the individual;

(ii)is authorized by UK Applicable Law to which BMC is subject and which also lays down suitable measures to safeguard the individual's rights and freedoms and legitimate interests; or

(iii) is based on the individual's explicit consent.

9.2 In the cases referred to in points (i) and (iii) of paragraph 9.1, BMC shall implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of BMC, to express his or her point of view and to contest the decision.

9.3 Decisions referred to in points (i) to (iii) of paragraph 9.1 shall not be based on special categories of Personal Information, unless the individual has given explicit consent or processing is necessary for reasons of substantial public interest, and suitable measures to safeguard the individual's rights and freedoms and legitimate interests are in place.

APPENDIX 2 - COMPLIANCE STRUCTURE

BMC has in place a compliance structure designed to ensure and oversee privacy compliance. This comprises four teams dedicated to ensuring effective governance of the Processor Policy and other privacy related policies, objectives and standards within BMC.

1. Executive Steering Committee

This committee consists of the three senior members of the BMC executive leadership having global responsibility for legal, compliance and ethics, human resources, information technology, security, business continuity management, privacy, and procurement. The role of the Executive Steering Committee is to provide senior executive governance and oversight of the Processor Policy, including:

(i) Ensuring that the Processor Policy and other privacy related policies, objectives and standards are defined and communicated.

(ii) Providing clear and visible senior management support and resources for the Processor Policy and for privacy objectives and initiatives in general.

(iii) Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Processor Policy, strategic plans, business objectives and regulatory requirements.

(iv) Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.

(v) Investigating, monitoring and annually reporting on compliance at a global and at a local scale.

(vi) Ensuring that BMC's business objectives align with the Processor Policy and related privacy and information protection strategies, policies and practices.

(vii) Facilitating communications on the Processor Policy and privacy topics with the BMC Executive Leadership Team and Board of Directors.

(viii) Instigating and assisting in determining the scope of audits of compliance with the Processor Policy, as described in the Processor Data Protection Binding Corporate Rules of BMC Software Audit Protocol in Appendix 4 ("Audit Protocol").

2. Project Working Group

The Project Working Group consists of mid-level executives (Vice Presidents and Directors) from key functional areas where Personal Information is processed, including human resources, legal, compliance and ethics, internal controls and assurance, customer support, information technology, information security, sales, marketing, finance, consulting services, education services, order management, research and development, global security and Group privacy.

The Project Working Group is responsible for:

(i) Promoting the Processor Policy at all levels in their organizations.

(ii) Facilitating in-depth reviews of business processes for assessing compliance with the Processor Policy as necessary.

(iii) Ensuring that BMC's business objectives align with the Processor Policy and related privacy and information protection strategies, policies and practices.

(iv) Assisting the Core Privacy Team in identifying, evaluating, prioritizing, and driving remedial actions consistent with BMC's policies and regulatory requirements.

(v) Implementing decisions made by the Executive Steering Committee within BMC on a global scale.

3. Core Privacy Team

This team has primary responsibility for ensuring that BMC complies with the Processor Policy and with global privacy regulations on a day to day basis. The group consists of the most senior BMC employee in each of the following functional areas: Group Data Protection Officer, EMEA Legal, Internal Assurance, IT and Information Security.

The role of the Core Privacy Team involves managing compliance with the day-to-day aspects of the Processor Policy and BMC's privacy initiatives including:

(i) Responding to inquiries and complaints relating to the Processor Policy from individuals, assessing the collection and processing of Personal Information by Group Members for potential privacy-related risks and identifying and implementing processes to address any areas of non-compliance.

(ii) Working closely with appointed local compliance officers in driving the Processor Policy and related policies and practices at the local country level, providing guidance and responding to privacy questions and issues.

(iii) Providing input on audits of the Processor Policy, coordinating responses to audit findings and responding to inquiries of the Commission.

(iv) Monitoring changes to global privacy laws and ensuring that appropriate changes are made to the Processor Policy and BMC's related policies and business practices.

(v) Promoting the Processor Policy and privacy awareness across business units and functional areas through privacy communications and training.

(vi) Evaluating privacy processes and procedures to ensure that they are sustainable and effective.

(vii) Investigating, monitoring and reporting periodically on the status of the Processor Policy at a global level and at a local level to the Executive Steering Committee.

(viii) Hosting and coordinating meetings of the Project Working Group.

(ix) Overseeing training for employees on the Processor Policy and on data protection legal requirements

in accordance with the requirements of The Controller and Processor Data Protection Binding Corporate Rules of BMC Software Privacy Training Requirements.

(x) Escalating issues relating to the Processor Policy to the Project Working Group and Executive Steering Committee where required.

(xi) Ensuring that the commitments made by BMC in relation to updating, and communicating updates to the Processor Policy as set out in the Processor Data Protection Binding Corporate Rules of BMC Software Updating Procedure, are met.

4. Local privacy champions network

BMC has established a network of local privacy champions to assist with the operation of the Processor Policy at country level. The role of the local privacy champions is to:

(i) Assist the Core Privacy Team with the implementation and management of the Processor Policy in their jurisdiction.

(ii) Escalate questions and compliance issues relating to the Processor Policy to the Core Privacy Team.

(iii) Oversee handling of local complaints from individuals.

(iv) Monitoring training and compliance at a local level.

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS

1. Background

1.1. The Processor Policy provides a framework for the transfer of Personal Information between BMC group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how BMC trains such individuals on the requirements of the Processor Policy.

1.2. BMC's Compliance and Ethics Office and the Group Data Protection Officer have overall responsibility for compliance and ethics training within BMC, including the delivery of BMC's formal privacy online training modules. Training on the Processor Policy is overseen by BMC's Core Privacy Team as 'subject matter experts', supported by the Compliance and Ethics Office.

1.3. Employees who have permanent or regular access to Personal Information, who are involved in the collection of Personal Information or in the development of tools to process Personal Information receive additional, tailored training on the Processor Policy and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis. Similarly, employees responsible for specific areas of compliance with the Processor Policy, such as responding to individuals' rights requests or handling complaints, receive specific training in these areas.

1.4. Contractors and/or contingent workers who have access to Personal Information are delivered adequate privacy training by their employers. Contractors and/or contingent workers' employers are contractually bound by their service agreements with BMC and by BMC's Third Party Code of Conduct, to deliver such adequate training.

2. Overview of training at BMC

2.1. Compliance and Ethics Training at BMC is carried out on a quarterly basis and covers a range of subjects, including data privacy, confidentiality and information security. Each year, one quarter's training is devoted to BMC's Code of Conduct (the "**Code**").

2.2. In addition to the quarterly training described in section 2.1, BMC also provides specific training on the Processor Policy as described in section 4 below.

3. Aims of data protection and privacy training at BMC

3.1.1. The aim of BMC's privacy training is to ensure that:

3.1.2. employees have an understanding of the basic principles of data privacy, confidentiality and information security;

3.1.3. employees understand the Code; and

3.1.4. employees in positions having permanent or regular access to Personal Information, who are involved

in the collection of Personal Information or in the development of tools to process Personal Information, receive appropriate training, as described in section 4, to enable them to process Personal Information in accordance with the Processor Policy.

3.1.5. General data protection and privacy training for new joining employees

3.1.6. New employees must complete BMC's Compliance and Ethics Office training on the Code, information security, and data privacy shortly after joining BMC. The Code requires employees to follow BMC's relevant data protection and privacy policies.

3.1.7. General data protection and privacy training for all employees

3.1.8. Employees worldwide receive periodic training on data protection and privacy as part of the Compliance and Ethics training process. This training covers basic data privacy rights and principles and data security in line with the requirements of the Processor Policy. It is designed to be both informative and user-friendly, generating interest in the topic. Completion of the course is monitored and enforced by BMC's Compliance and Ethics Office and employees must correctly answer a series of multiple choice questions for the course to be deemed complete.

3.1.9. All employees also benefit from:

(a) all Compliance and Ethics training modules, including data protection modules, which can be accessed online at any time; and

(b) ad-hoc communications consisting of emails, awareness messaging placed on BMC intranet pages, and information security posters displayed in offices which convey the importance of information security and data protection issues relevant to BMC, including for example, social networking, remote working, engaging data processors and the protection of confidential information.

4. Training on the Processor Policy

4.1 BMC's training on the Processor Policy will cover the following main areas and employees receive training appropriate to their roles and responsibilities within BMC:

4.1.1 Background and rationale:

(a) What is data protection law?

(b) How data protection law practically affects BMC in relation to data transfers from the UK

(c) The scope of the Processor Policy

(d) Terminology and concepts

4.1.2 The Processor Policy:

(a) An explanation of the Processor Policy

(b) Practical examples

(c) The rights that the Processor Policy gives to individuals

4.1.3 Where relevant to an employee's role, training will cover the following procedures under the Processor Policy:

(a) Individuals' Rights Requests Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

(f) Data breach handling

5. Further information

5.1 Any queries about training under the Processor Policy should be addressed to the Compliance and Ethics Office which can be contacted by email at: compliance_ethicsoffice@bmc.com.

APPENDIX 4 - AUDIT PROTOCOL

1. Background

1.1 The purpose of the Processor Policy is to safeguard Personal Information transferred between the BMC Group Members.

1.2 The Processor Policy requires approval from the Commission. One of the requirements of the Commission is that BMC audits compliance with the Processor Policy and satisfies certain conditions in so doing and this document describes how BMC deals with such requirements.

1.3 One of the roles of BMC's **Core Privacy Team** is to provide guidance about the collection and processing of Personal Information subject to the Processor Policy and to assess the collection and processing of Personal Information by Group Members for potential privacy-related risks. The collection and processing of Personal Information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by BMC to ensure compliance with the Processor Policy as required by the Commission, this is only one way in which BMC ensures that the provisions of the Processor Policy are observed and corrective actions taken as required.

2. Approach

Overview of audit

2.1.1 Compliance with the Processor Policy is overseen on a day to day basis by the **Core Privacy Team**, consisting of **BMC's Group Data Protection Officer**; **BMC's Vice President, EMEA General Counsel**; **BMC's Vice President Assurance, Risk & Ethics** and **BMC's Global Security Services Director**.

2.1.2 BMC's **Assurance Department** (consisting of **Internal Audit**, **Internal Controls**, and **IT Assurance** functions) will be responsible for performing and/or overseeing independent audits of compliance with the Processor Policy and will ensure that such audits address all aspects of the Processor Policy in accordance with the BMC audit program. All Group Members are subject to the BMC audit program and shall comply with any audit process initiated by BMC's Assurance Department. BMC's **Assurance Department** will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of BMC's **Core Privacy Team** and the **Executive Steering Committee** and that any corrective actions to ensure compliance take place within a reasonable timescale.

2.2Timing and scope of audit Audit of the Processor Policy will take place:

(a) at least **annually** in accordance with BMC's **corporate audit program**;
(b) at the request of BMC's **Core Privacy Team** or the **Executive Steering Committee**; and/or
(c) as determined necessary by the **Assurance Department**.

2.2.2 To the extent that a Group Member processes Personal Information on behalf of a third party controller, audit of the Processor Policy will also take place as required under the contract in place between that Group Member and that third party controller.

2.2.3 The scope of the audit program will cover all aspects of the Processor Policy, including methods of ensuring that corrective actions will take place. Such aspects may include applications, IT systems, databases that process Personal Information, onward transfers, decisions taken as regards mandatory requirement under national laws that conflicts with the Processor Policy, review of the contractual terms used for the transfers out of the Group, and corrective actions. The scope of each audit will be determined by BMC's **Assurance Department** with consideration given to input received from the **Core Privacy Team** and **Executive Steering Committee** based on the use of a risk-based analysis which will consider relevant criteria, for example: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of the Personal Information processed.

2.2.4 In the event that a third party controller on whose behalf BMC processes Personal Information exercises its right to audit BMC for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities and activities relating to that controller. BMC will not provide a controller with access to systems which process Personal Information of other controllers.

2.3 Auditors

2.3.1 t of the Processor Policy will be undertaken by BMC's **Assurance Department** and BMC may utilize other accredited internal/external auditors as determined by BMC.

2.3.2 In the event that a third party controller on whose behalf BMC processes Personal Information exercises their right to audit BMC for compliance with Part II of the Processor Policy, such audit may be undertaken by that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between BMC and that controller.

2.3.3 BMC's **Audit Committee** consisting of members of the Board of Directors of BMC Software, Inc. (the "**Board**") is appointed by the Board to assist it in fulfilling its oversight responsibilities with respect to matters including BMC's legal and regulatory compliance and the performance of internal audit functions and external auditors.

2.3.4 The **Audit Committee** is independent and reports regularly to the Board on its findings and recommendations, including in relation to the performance of external auditors and BMC's internal audit function.

2.3.5 BMC will also cooperate with any audit requests from the Commission in accordance with the Cooperation Procedure in Appendix 6.

2.4 Report

2.4.1 BMC's Assurance Department will provide the results of any audit of the Processor Policy to BMC's Core Privacy Team, the Executive Steering Committee and other appropriate management personnel. The Assurance Department will also provide a summary of the audit results to the Audit Committee, which reports directly to the Board.

Upon request, BMC shall:

(a) provide copies of the results of any audit of the Processor Policy to the Commission; and

(b) to the extent that an audit relates to Personal Information processed by BMC on behalf of a third party controller, make the results of any audit of compliance with the Processor Policy available to that controller, as set out in the contract between BMC and that controller.

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE

1. Introduction

1.1 The Processor Policy safeguards Personal Information processed or transferred between the BMC Group Members. The purpose of this Complaint Handling Procedure is to explain how complaints brought by a UK Individual whose Personal Information is processed by BMC under the Processor Policy are dealt with.

2. How UK Individuals can bring complaints UK Individuals who are third party beneficiaries of this Processor Policy can bring complaints in writing by contacting BMC's Group Data Protection Officer or by emailing privacy@bmc.com. These are the contact details for all complaints made under the Processor Policy.

Maxime Roze
Group Data Protection Officer
Phone: +33 (0)1.57.00.62.60
Email: privacy@bmc.com
Address: Cœur Défense - Tour A, 10ème étage, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, FRANCE

3. Who handles complaints?

3.1 Where a complaint is brought in respect of the collection and processing of Personal Information where BMC is the processor in respect of that information, BMC will communicate the details of the complaint to the Client promptly and will act strictly in accordance with the terms of the contract between the Client and BMC if the Client requires that BMC investigate the complaint.

By derogation to the aforementioned, when a Client has disappeared factually, no longer exists in law or has become insolvent, BMC's Group Data Protection Officer will handle complaints in accordance with this section 3.2.

BMC's Group Data Protection Officer will acknowledge receipt of a complaint to the UK Individual concerned within 5 working days, investigating and making a substantive response within one month.

If, due to the complexity of the complaint or the number of received complaints, a substantive response cannot be given within this period, BMC's Group Data Protection Officer will advise the complainant accordingly and provide a substantive response within a reasonable timeframe (not exceeding two additional months).

If the complainant disputes the response of the Group Data Protection Officer (or the individual or department

within BMC tasked by the Group Data Protection Officer with resolving the complaint) or any aspect of a finding, and notifies the Group Data Protection Officer accordingly, the matter will be referred to the Vice President EMEA General Counsel who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Vice President EMEA General Counsel will respond to the complainant within six months of the referral. As part of the review, the Vice President EMEA General Counsel may arrange to meet the parties in an attempt to resolve the complaint. If the complaint is upheld, the BMC Vice President EMEA General Counsel will arrange for any necessary steps to be taken as a consequence. Such necessary steps may include payment of compensation or other forms of redress (correction of mistake, retraction, apology, etc.) as well as the implementation of corrective actions made necessary in light of the additional review by BMC Vice President EMEA General Counsel.

Any arrangements to meet with the complainants shall not incur any costs for the complainants nor influence their ability to exercise their rights. Any inability or declination to meet on the part of the complainant shall not impair the fair and appropriate handling of the complaint.

UK Individuals whose Personal Information is processed subject to UK Data Protection Law also have the right to lodge a complaint to the Commission and/or to lodge a claim with a UK court whether or not they have first made a complaint to BMC and without having exhausted this Complaints Handling Procedure.

APPENDIX 6 - COOPERATION PROCEDURE

1. Introduction

This Cooperation Procedure sets out the way in which BMC will cooperate with the Commission in relation to the Processor Policy. BMC's Group Data Protection Officer will be the primary point of contact responsible for liaising with the Commission under the Cooperation Procedure.

2. Cooperation Procedure

2.1 Where required, BMC will make the necessary personnel available for dialogue with the Commission in relation to the Processor Policy.

2.2 BMC will actively review and consider any decision made by the Commission on any data protection law issues that may affect the Processor Policy, and comply with any guidance published by the Commission in connection with BCR for processors.

2.3 The Commission will, without restrictions, be provided with any audit reports of the Processor Policy upon request.

2.4 BMC agrees that:

2.4.1 where any BMC Group Member is located in the UK, BMC agrees that the Commission may audit that Group Member for the purpose of reviewing compliance with the Processor Policy, in accordance with UK Applicable Law; and

2.4.2 in case of a Group Member located outside the UK, BMC agrees that the Commission may audit that Group Member for the purpose of reviewing compliance with the Processor Policy in accordance with UK Applicable Law

2.5 BMC will consider any communication or recommendations from the Commission and will comply with any formal decisions or notices of the Commission in relation to the interpretation of and the application of BCRs. BMC may appeal any final decision of the Commission in accordance with UK Applicable Law.

APPENDIX 7 - UPDATING PROCEDURE

1. Introduction

1.1 This Updating Procedure sets out the way in which BMC will communicate changes to the Processor Policy to the Commission, individuals, its clients and to the BMC Group Members bound by the Processor Policy.

1.2 BMC's Group Data Protection Officer will keep a fully updated list of the Group Members and of the sub-processors involved in the data processing activities for the controller which shall be made accessible to the data controller, individuals and the Commission.

1.3 BMC's Group Data Protection Officer will keep track of and record any updates to the rules and provide the necessary information systematically to the data controller and upon request to the Commission.

1.4 No transfer is made to a new Group Member until the new Group Member is effectively bound by the Processor Policy and can deliver compliance.

2. Material changes to the Processor Policy

2.1 BMC will promptly communicate any material changes to the Processor Policy (such as those that potentially affect the data protection compliance, are potentially detrimental to individual rights, potentially affect the level of the protection offered by the Processor Policy, or affect the binding nature of the Processor Policy) to the Commission and all Group Members. Material changes will be communicated to the Commission at least once a year.

2.1 Where a change to the Processor Policy materially affects the conditions under which BMC processes Personal Information on behalf of any Client under the terms of its contract with BMC, BMC will also communicate such information to any affected Client with sufficient notice to enable affected Clients to object before the modification is made. BMC's Client may then suspend the transfer of Personal Information to BMC and/or terminate the contract, in accordance with the terms of its contract with BMC.

3. Administrative changes to the Processor Policy

3.1 BMC will communicate changes to the Processor Policy which are administrative in nature (including changes in the list of Group Members) to the Group Members regularly and the Commission at least once a year. BMC will also provide a brief explanation to the Commission of the reasons for any notified changes to the Processor Policy.

3.2 BMC will make available changes to the Processor Policy which are administrative in nature (including changes in the list of Group Members) to any Client on whose behalf BMC processes Personal Information.

4. Communicating and logging changes to the Processor Policy

4.1 The Processor Policy contains a change log which sets out the date of revisions to the Processor Policy and the details of any revisions made. BMC's Group Data Protection Officer will maintain an up to date list of the changes made to the Processor Policy.

4.2 BMC will communicate all changes to the Processor Policy, whether administrative or material in nature:

4.2.1 to the Group Members which shall be automatically bound by such changes; and

4.2.2 systematically to Clients on whose behalf BMC processes Personal Information and individuals who benefit from the Processor Policy via bmc.com.

5. New Group Members

5.1 BMC's Group Data Protection Officer will ensure that all new Group Members are bound by the Processor Policy before a transfer of Personal Information to them takes place.

APPENDIX 8 - MATERIAL SCOPE OF THE PROCESSOR POLICY

1. Introduction

1.1 BMC's Processor Policy provides a framework for the transfer of Personal Information between BMC Group Members.

1.2 This document sets out the material scope of the Processor Policy. It specifies a non-exhaustive list of data transfers or set of transfers, including the nature and categories of Personal Information, the type of processing and its purposes, the types of individuals affected, and the identification of the third country or countries.

1.3 Personal information transferred or accessed from overseas entities is minimized and limited to that required for the purpose.

2.1 Customer relationship data (Sales & Marketing)

Who transfers the Personal Information described in this section?	*A Group Member may transfer the Personal Information that they control described in this section to every other BMC Group Member.*
Who receives this Personal Information?	*Every BMC Group Member may receive the Personal Information described in this section which is sent to them by any other BMC Group Member.*
What categories of Personal Information are transferred?	*- Contact Information, such as address, contact telephone numbers (landline and mobile) and personal email address, and;* *- Employment information, such as job title, roles and company.*
What Sensitive Personal Information (if any) is transferred?	*BMC does not collect or otherwise process Sensitive Personal Information.*
Who are the types of individuals whose Personal Information is transferred?	*Sales prospects and customers.*
Why is this Personal Information transferred and how will it be processed?	*Sales and Marketing activities are managed both at local, regional and global levels, for the purposes and in accordance with the lawful basis described below:* *Engage in and process transactions (Lawful basis: BMC's legitimate interest);* *Use BMC customers relationship management systems (Lawful basis: BMC's legitimate interest);* *Manage customers clickwrap acceptance of BMC's license agreements (Lawful basis: BMC's legitimate interest);* *Review bid processes (Lawful basis: BMC's legitimate interest);*

	Respond to inquiries and requests (Lawful basis: BMC's legitimate interest); *Provide information on BMC products and services, on BMC's partners offering and BMC's services and products (Lawful basis: BMC's legitimate interest or consent as the case may be);* *Manage export compliance (Lawful basis: BMC's legitimate interest);* *Send satisfaction survey (Lawful basis: BMC's legitimate interest); or* *Process orders for billing, booking, accounting and invoicing purposes (Lawful basis: BMC's legitimate interest).*
Where is this Personal Information processed?	*The Personal Information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9.*

2.2 **Human Resources data**

Who transfers the Personal Information described in this section?	*A Group Member may transfer the Personal Information that they control described in this section to every other BMC Group Member.*
Who receives this Personal Information?	*Every BMC Group Member may receive the Personal Information described in this section which is sent to them by any other Group Member.*
What categories of Personal Information are transferred?	*- Personal Identification, such as first name, second name and date of birth;* *- Contact Information, such as home address, contact telephone numbers (landline and mobile) and personal email address;* *- Education & Skills, such as employment and education history including qualifications, job application, employment references;* *- Family Information, such as emergency contacts and contact information;* *- Employment Information, such as job title, start and leave dates, employment contract and promotions, performance reviews and ratings, details of any leave, disciplinary records, training history and development needs;* *- Criminal Personal Information, to the extent authorized by domestic law;* *- User Account Information, such as employee ID and credentials,* *- Geographical Information, such as location of employment;* *- Financial Information, including compensation, payroll, benefits, expenses or other payments claimed and bank account details;* *- Government Identifiers, such as passport and national ID;* *- Citizenship or Immigration Status;* *- IT systems monitoring, such as logs; and* *- Photos and CCTV images.*

What Sensitive Personal Information (if any) is transferred?	• *Health information, such as accident records and health management questionnaires, to the extent authorized by domestic law. Such Personal Information is collected and otherwise processed in accordance with Article 6 and 9 of UK GDPR. Health information is subject to an obligation of secrecy under domestic law. Processing of health information is necessary for the purposes of:* ○ *carrying out the obligations and exercising specific rights of BMC in the field of employment and social security and social protection law in so far as it is authorised by domestic law;* ○ *preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law.* • *Criminal Personal Information, to the extent authorized by domestic law. Processing of criminal offence information is necessary for the purpose of criminal record checks. Such Personal Information is collected and otherwise processed in accordance with Article 6 and 10 of UK GDPR.*
Who are the types of individuals whose Personal Information is transferred?	*Applicants and employees (both current and former).*
Why is this Personal Information transferred and how will it be processed?	*BMC has approximately 250 employees in the UK. HR activities are managed both at local, regional and global levels, for the purposes and in accordance with the lawful basis described below:* *- Administer employment, including employment verifications and background checks, delivery of employment and travel letters, regulatory reporting, training, administration of lunch vouchers, internal reporting, resolution of employee requests, leave management, assistance with immigration and visa processing, new hire provisioning, candidates*

	sourcing on social networks, performance assessments (Lawful basis: BMC's legitimate interest or performance of a contract with the individual as the case may be); *- Administer compensation and benefits, including salary, bonuses, long term incentive programs, health, welfare and retirement plans (Lawful basis: Performance of a contract with the individual);* *- Manage payroll, including employee pay checks, benefit deductions, payroll taxes, direct deposit, garnishments/levies/child support, exception pay (bonuses, commissions, etc.), hours worked, final pay, unused PTO pay-out, leaves of absence (Lawful basis: Performance of a contract with the individual);* *- Administer corporate credit card program and reimburse business expenses (Lawful basis: BMC's legitimate interest);* *- Protect employee safety and security, including travels, office & parking access control, assistance in case of a medical emergency, CCTV (Lawful basis: BMC's legitimate interest or compliance with a legal obligation as the case may be);* *- Assign desks, drawers and corporate devices such as mobiles and laptops (Lawful basis: BMC's legitimate interest);* *- Provide IT tools and services to employees, including email and other collaboration tools (Lawful basis: BMC's legitimate interest);* *- Ensure secure use of IT tools and services, including identity federation, email and outbound file transfer protections, endpoint protection, cloud service monitoring, cybersecurity logging and forensics (Lawful basis: BMC's legitimate interest);* *- Monitor business mobile costs (Lawful basis: BMC's legitimate interest);* *- Provide company lease cars and fuel cards (Lawful basis: BMC's legitimate interest);*

	- Make business travel arrangements (Lawful basis: BMC's legitimate interest); *- Support internal and external communications, including employee communications, surveys, events and challenges (Lawful basis: BMC's legitimate interest);* *- Maintain BMC organizational charts (Lawful basis: BMC's legitimate interest);* *- Issue emergency communications and maintain business continuity in case of an emergency situation, including relocation to recovery site (Lawful basis: BMC's legitimate interest);* *- Perform financial planning, accounting and tax management (Lawful basis: BMC's legitimate interest);* *- Support the delivery of BMC products & services to customers, including use of IT tools and resources to administer, maintain and support such products & services (Lawful basis: BMC's legitimate interest);* *- Comply with applicable laws & regulations, including anti-discrimination, privacy, export control, and Know Your Customer ("KYC") banking requirements for company directors and bank account signers (Lawful basis: Compliance with a legal obligation);* *- Interact with local works councils (Lawful basis: Compliance with a legal obligation);* *- Monitor compliance with company policies and procedures, including training, internal controls, assessments, questionnaires, testing and BMC Ethics Helpline (Lawful basis: BMC's legitimate interest);* *- Protect BMC interests in contentious and non-contentious legal matters, which includes HR performance management and discipline, litigation holds, investigations, patents registration, contract negotiations, the*

	performance of audits and compliance training (Lawful basis: BMC's legitimate interest); and *- support other business and employment-related activities (Lawful basis: BMC's legitimate interest).*
Where is this Personal Information processed?	*BMC has approximately 250 employees in the UK. HR activities are managed both at local, regional and global levels.* *The Personal Information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9.*

2.3 **Supplier / Vendor data**

Who transfers the Personal Information described in this section?	*A Group Member may transfer the Personal Information that they control described in this section to every other BMC Group.*
Who receives this Personal Information?	*Every BMC Group Member may receive the Personal Information described in this section which is sent to them by any other Group Member.*
What categories of Personal Information are transferred?	*Personal details;* *Contact details;* *Goods and services provided;* *Financial details;* *Employment information;* *Education and training details.*
What Sensitive Personal Information (if any) is transferred?	*BMC does not collect or otherwise process Sensitive Personal Information.*
Who are the types of individuals whose Personal Information is transferred?	*Suppliers / Vendors*
Why is this Personal Information transferred and how will it be processed?	*Supplier management activities are performed both at local, regional and global levels, for the purposes and in accordance with the lawful basis described below:* *Procurement management, including supplier selection and due diligence activities (Lawful basis: BMC's legitimate interest);*

	Engage in and process transactions (Lawful basis: BMC's legitimate interest); *Use BMC supplier management systems (Lawful basis: BMC's legitimate interest);* *Manage supplier acceptance of BMC's agreements (Lawful basis: BMC's legitimate interest);* *Respond to inquiries and requests (Lawful basis: BMC's legitimate interest);* *Manage export compliance (Lawful basis: Compliance with a legal obligation);* *Process supplier orders for payment purposes (Lawful basis: BMC's legitimate interest).*
Where is this Personal Information processed?	*The Personal Information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9.*

3. Business Partners / Resellers data

Who transfers the Personal Information described in this section?	*A Group Member may transfer the Personal Information that they control described in this section to every other BMC Group Member.*
Who receives this Personal Information?	*Every BMC Group Member may receive the Personal Information described in this section which is sent to them by any other Group Member.*
What categories of Personal Information are transferred?	*Personal details;* *Contact details.*
What Sensitive Personal Information (if any) is transferred?	*BMC does not collect or otherwise process Sensitive Personal Information.*
Who are the types of individuals whose Personal Information is transferred?	*Business Partners / Resellers*
Why is this Personal Information transferred and how will it be processed?	*Partner management activities are performed both at local, regional and global levels, for the purposes and in accordance with the lawful basis described below:* *Performing sales, support, consulting services, training, research and development, and marketing activity (Lawful basis: BMC's legitimate interest or consent as the case may be).*
Where is this Personal Information processed?	*The Personal Information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9.*

APPENDIX 9 - LIST OF BCR GROUP MEMBERS

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
United Kingdom	BMC Software Limited	01927903	13th floor, 1 Angel Court, EC2R 7HJ London, United Kingdom	Privacy@bmc.com	Categories of data listed in Appendix 8.
Austria	BMC Software GmbH	FN 12295 k	Teinfaltstraße 8, Vienna, 1010, Austria		
Belgium	BMC Software Belgium NV	BE 424902956	Botanic Tower, Boulevard Saint-Lazare, 4-10, 1210, Belgium		
Denmark	BMC Software A/S	DK 13115885	H.C. Andersens Boulevard 38, 3. TH., 1553 Kobenhavn V , Denmark		
Finland	BMC Software OY	735091	c/o Anyspace, Hämeentie 135 A, 00560, Finland		
France	BMC Software France SAS	313400681	Coeur Défense, 100, Esplanade du Général de Gaulle, 10th Floor Tower A, 92400 Courbevoie, France		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Germany	BMC Software GmbH	HRB 24281	Wiesenhüttenstr. 11,60329 Frankfurt am Main, Germany	Privacy@bmc.com	Categories of data listed in Appendix 8
Greece	BMC Software Hellas MEPE	9300937852	1 Alamanas & Delfon, 15125 Marousi, Greece		
Ireland	BMC Software Ireland Unlimited	481578	3 The Campus, Cherrywood,Dublin 18, D18 TF72, Ireland		
Italy	BMC Software S.r.l	1222185	Corso Vercelli 40, Milan, 20145, . Italy		
Norway	BMC Software AS	AS-979803125	Hagaløkkveien 26, 1383 Asker, Norway		
Poland	BMC Software Sales (Poland) Sp.z.o.o.	18835	Zlota 59, Office #602 Warszawa, Polska, 00-120		
Portugal	BMC Software Portugal Soc. Unipessoal Lda	503870447	Avenida Duque d´Ávila, nº 46, 3 C 1050-083 Lisbon, Portugal		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Spain	BMC Software S.A.	A79305389	Parque Empresarial La Finca, Paseo del, Club Deportivo 1, Edificio 17, Planta Baja, Izquierda, 28223 Pozuelo de Alarcón, Madrid, Spain	Privacy@bmc.com	.
Sweden	BMC Software AB	556207-5795	Vasagatan 38, Stockholm, SE- 111 20, Sweden		
Switzerland	BMC Software GmbH	CH020.4.002.762 -1	Talstrasse 83, 8001 Zürich, Switzerland		
The Netherlands	BMC Software Distribution B.V.	30106755	Boeingavenue 220, 1119PN Schiphol-Rijk, The Netherlands		Categories of data listed in Appendix 8
Argentina	BMC Software de Argentina S.A.	1694851	Ing. Butty 220 - Piso 18 Capital Federal, Buenos Aires, C1001AFB, Argentina		
Australia	BMC Software (Australia) Pty. Ltd.	ABN12 007 280 088	Level 13/383, Kent Streeet, Sydney, NSW 2000, Australia		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Brazil	BMC Software do Brasil Ltda.	00.723.020/0001-90	Av. Rebouças 3.970 e Av. Dra Ruth Cardoso, 8.501, 22º Andar, Pinheiros, São Paulo, SP 05425-070	Privacy@bmc.com	Categories of data listed in Appendix 8
Canada	BMC Software Canada Inc.	1654693	150 King Street West, Suite 306-02, Toronto, Ontario, Canada		
China	BMC Software (China) Limited	91110101600086987G	Level 38, China World Tower B, No.1, Jianguomenwai Avenue, Chaoyang District, Beijing, 100004, China		
	Branch Office of BMC Software (China) Limited	913101150878080016	Unit 2101, The Platinum, No. 233 Taicang Road, Huangpu District, Shanghai 200020, China		
Colombia	BMC Software Colombia SAS	01848479	Carrera 9 N°115-06/30, Tierra Firme Complex, Tierra Firme Tower, 17th Floor, Bogotá, D.C. 110111, Colombia		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Dubai	BMC Software Limited - Dubai Branch	505326	U-Bora Commercial Tower, Building No.2, Business Bay, 40th Floor, Unit 4003, Dubai, United Arab Emirates	Privacy@bmc.com	Categories of data listed in Appendix 8
Hong Kong	BMC Software (Hong Kong) Limited	543682	Level 23, One Island East, No.18 Westlands Road, Taikoo Place, Quarry Bay, Hong Kong		
India	BMC Software India Private Limited	CIN U 72200 PN 2001 PTC 16290	Wing 1, Tower 'B', Business Bay, Survey No. 103, Hissa No. 2, Airport Road, Yerwada, Pune, Maharashtra 411006		
Israel	BMC Software Israel LTD	52-003784-7	10 Habarzel Street, P. O. Box 58168, 6158101, Tel Aviv, Israel		
Japan	BMC Software K.K. (Japan)	3011201009842	Harmony Tower 24F, 1-32-2 Honcho, Nakano-ku, Tokyo, 164-8721		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Korea	BMC Software Korea, Ltd.	110111-1285877	9 FL Two IFC, 10 Gukjekeumyung-ro, Youngdeungpogu, Seoul 07326, South Korea	Privacy@bmc.com	Categories of data listed in Appendix 8.
Malaysia	BMC Software Asia Sdn Bhd	199901024358	Level 15, 1 First Avenue 2A Dataran Bandar Utama Damansara, 47800 Petaling Jaya, Malaysia		
Mexico	BMC Software de Mexico, S.A. de C.V.	Mercantile Folio 248373	Volcán 150, Piso 2, Oficina 202, Colonia Lomas de Chapultepec I Sección, Alcaldía Miguel Hidalgo, C.P. 11000, Cd. de México, México		
	BMC Software Distribution de Mexico, S.A. de C.V.	Mercantile Folio 271309	Volcán 150, Piso 2, Oficina 202, Colonia Lomas de Chapultepec I Sección, Alcaldía Miguel Hidalgo, C.P. 11000, Cd. de México, México		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
New Zealand	BMC Software (New Zealand) Limited	28 009 503	Level 2, 40 Lady Elizabeth Lane, Wellington Central, Wellington, 6011, New Zealand	Privacy@bmc.com	Categories of data listed in Appendix 8.
Saudi Arabia	The Branch of BMC Software Limited	1010297290	Al-Deghaither Center, Tahliyah Street, 11451 Riyadh, Kingdom of Saudi Arabia		
	BMC Software Limited Regional Headquarters Branch	7054054189	Al-Deghaither Center, Tahliyah Street, 11451 Riyad, Kingdom of Saudi Arabia		
South Africa	BMC Software Limited (Incorporated in England) - Branch entity	1927903	2 Conference Lane, Bridgewater One, Block 1, Bridgeway Precinct, Century City, 7446, South Africa		
Singapore	BMC Software Asia Pacific Pte. Ltd.	199504342D	600 North Bridge Road #20-01/10 Parkview Square, 188778, Singapore,		
Taiwan	Tawain Representative Office of BMC Software (Hong Kong) Limited	28986710	11/F, 1172/1173, No.1, Songzhi Rd., Taipei, 11047, Taiwan		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Thailand	BMC Software (Thailand) Limited	(3)82/2543	63 Wireless Road Level 23, Athenee Tower Pathumwan, Lumpini Bangkok, 10330, Thailand	Privacy@bmc.com	Categories of data listed in Appendix 8.
United States	BMC Helix Federal, LLC	10024034	1209, Orange Street, c/o The Corporation Trust Company, Corporation Trust Center, 19801, Wilmington, Delaware, USA		
	BMC Software, Inc.	DE Charter # - 2165371			

APPENDIX 10 - LIST OF DEFINITIONS

For the purposes of this Policy and unless otherwise specified, the following terms have the meaning set forth below:

"**Client**" or "**Controller**" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information and instructs BMC to collect, process and transfer such Personal Information under a contract evidenced in writing.

"**Commission**" means the UK Information Commission.

"**Controller Policy**" means the UK Controller Data Protection Binding Corporate Rules of BMC Software.

"**Group Members**" or "**BMC**" means BMC group members listed on in Part III, Appendix 9 of the Processor Policy.

"**Personal Information**" means any information relating to an identified or identifiable living individual, in line with the definition of "personal data" in the UK Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK GDPR**") as incorporated into and amended by the European Union (Withdrawal) Act 2018 as amended or superseded from time to time (together, "**UK Data Protection Law**").

"**Procedure**" means the Individuals' Rights Requests Procedure described in Part III Appendix 1 of the Processor Policy.

"**Processing**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor Policy**" means the UK Processor Data Protection Binding Corporate Rules of BMC Software

"**Request**" means an individual's rights request relating to Personal Information collected, processed or transferred by BMC as a processor, as described in Part III Appendix 1 of the Processor Policy.

"**UK Applicable Law**" means all UK laws, regulations, statutes or any other rules applicable to BMC.

"**UK Group Member**" means BMC Software Ltd.

"**UK Individuals**" means individuals meeting the criteria described in Article 3 of UK GDPR.

Article III. PART IV: DOCUMENT INFORMATION

Version	2.0
Origination Date:	April 1, 2024
Last Modified Date:	October 1, 2026
Modified by:	Maxime Roze, Chief Privacy Officer & Group Data Protection Officer
Next Review Date:	September 30, 2027