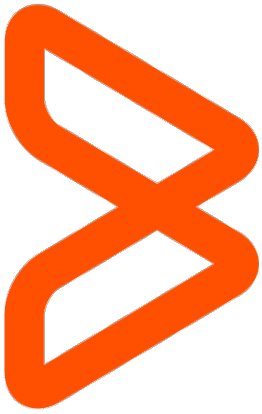

UK Controller Data Protection Binding Corporate Rules of BMC Software

bmc

TABLE OF CONTENTS

TABLE OF CONTENTS ____ 1

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 AS A CONTROLLER ____ 5

SECTION A: BASIC PRINCIPLES ... 5

SECTION B: PRACTICAL COMMITMENTS ... 12

SECTION C: THIRD-PARTY BENEFICIARY RIGHTS ... 16

PART III: APPENDICES ____ 18

APPENDIIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE ... 18

APPENDIX 2 - COMPLIANCE STRUCTURE ... 24

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS ... 27

APPENDIX 4 - AUDIT PROTOCOL ... 30

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE ... 32

APPENDIX 6 - COOPERATION PROCEDURE ... 34

APPENDIX 7 - UPDATING PROCEDURE ... 34

APPENDIX 8 - MATERIAL SCOPE OF THE CONTROLLER POLICY ... 36

APPENDIX 9 - LIST OF BCR GROUP MEMBERS ... 47

APPENDIX 10 - LIST OF DEFINITIONS ... 57

PART IV: DOCUMENT INFORMATION ____ 58

bmc

INTRODUCTION

These UK1 Controller Data Protection Binding Corporate Rules of BMC Software (the "**Controller Policy**") establish BMC Software's approach to compliance with UK Data Protection Law, including transfers of Personal Information between the BMC group members ("**Group Members**") listed in Part III, Appendix 9.

The Controller 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 the UK GDPR may be (i) transferred out of the UK by Group Members then processed by Group Members outside of the UK, for BMC's own purposes in respect of processing it undertakes as 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 Controller 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 Controller 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 Controller Policy applies to Personal Information of past, current, and potential employees, customers, resellers, suppliers, service providers, and other third parties, collected and processed in conjunction with BMC business activities and the administration of employment.

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

The Controller 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 is processed. 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. When BMC collects and processes the Personal Information of its past, current and potential employees, customers, resellers, suppliers, service providers and other third parties, this activity, and the Personal Information in question, is covered and regulated by UK Data Protection Law. 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 Controller Policy describes how BMC will comply with data protection law in respect of processing undertaken in its capacity **as a controller**. BMC also acts as a processor and has set out its commitments in its UK Processor Data Protection Binding Corporate Rules of BMC Software (the "**Processor 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 Controller 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.

BMC will apply the Controller Policy globally, and in **all cases** where BMC processes Personal Information as a controller, both manually and by automatic means, when the Personal Information relates to past, current and potential employees, customers, resellers, suppliers, service providers and other third parties. Additional details about the material scope of the Controller policy are set out in Appendix 8**.**

The Controller Policy applies to all Group Members and their employees worldwide, and requires that Group Members who collect, process or transfer Personal Information as a controller must comply with **Part II** of the Controller Policy together with the practical procedures set out in the appendices in **Part III** of the Controller

Policy, irrespective of the country in which they are located. The procedures and appendices are an integral part of this Controller Policy.

This Controller 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 Controller Policy, up to and including termination of employment. As for contractors and/or contingent workers, this Controller Policy is expressly referred to in their service agreement and violation of this Controller Policy can lead to termination of such service agreement.

FURTHER INFORMATION

If you have any questions regarding the provisions of the Controller Policy, your rights under the Controller 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 Controller Policy and ensuring that changes to the Controller Policy are notified, to the Group Members, 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 AS A CONTROLLER

The Controller Policy applies in all cases where a Group Member collects, processed and transfers Personal Information as a controller.

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

- **Section A:** addresses the basic principles of UK Data Protection Law that a Group Member must observe when it collects, processed and transfers Personal Information as a controller.
- **Section B:** deals with the practical commitments made by BMC to the Commission in connection with the Controller Policy.
- **Section C:** describes the third party beneficiary rights that BMC has granted to individuals under Part II of the Controller Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH THIRD COUNTRY NATIONAL LEGISLATION AND ACCOUNTABILITY

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

As an organization, BMC will comply with any applicable legislation relating to Personal Information, and will ensure that where Personal Information is collected and processed, this is done in accordance with the local law.

Where there is no law or the law does not meet the standards set out by the Controller Policy, BMC's position will be to process Personal Information adhering to the Controller Policy.

To the extent that any applicable data protection legislation requires a higher level of protection, BMC acknowledges that such applicable data protection legislation will take precedence over the Controller Policy.

Where BMC believes that applicable third country national legislation prevents it from complying with the Controller Policy, Rule 16A shall apply.

Rule 1B – BMC will demonstrate its compliance with the Controller Policy ("Accountability")

Pursuant to Article 30.1 of UK GDPR, BMC will maintain a record of processing activities carried under its responsibility in accordance with UK Applicable Law. This record shall be maintained in writing, including in an electronic form, and shall be made available to the Commission upon request.

In order to enhance compliance and where required, data protection impact assessments shall be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons. The data protection impact assessments process will be overseen by BMC's Group Data Protection Officer. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by BMC to mitigate the risk, BMC shall consult the Commission, prior to processing.

Appropriate technical and organisational measures will be implemented which are designed to make data protection principles effective and to facilitate compliance with the requirements set up by the Controller Policy in practice, taking into account the state of the art, cost of implementation, risks to data subjects, nature, scope, context and purpose of the processing (data protection by design and by default).

BMC will identify and implement such data protection principles when developing new IT systems, services, policies and processes that involve processing Personal Information, based on privacy by design and by default checklists.

BMC will carry out data protection impact assessments for processing activities likely to result in a high risk to the rights and freedoms of individuals and will consult the Commission, where required under the UK GDPR.

Pursuant to Articles 5.2 and 24 of UK GDPR, every entity acting as Controller shall be responsible for and be able to demonstrate compliance with the Controller Policy.

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

Rule 2A – BMC will explain to individuals how that information will be processed ("Transparency and fairness").

BMC will ensure that individuals are told in a clear and comprehensive way (usually by means of an easily accessible fair processing statement) how their Personal Information will be processed. The information BMC has to provide to individuals includes all information necessary in the circumstances to ensure that the processing of Personal Information is fair and transparent, including the following:

- the identity of the controller;
- the contact details of the Group Data Protection Officer;
- the purposes for which data will be processed;
- the legal basis for processing that data;
- who Personal Information will be shared with;
- countries outside of the UK Personal Information may be transferred to, and the safeguards in place to

protect it;

- the retention period for Personal Information;
- the individual rights guaranteed by BMC to request access to and rectification or erasure of Personal Information or restriction of processing concerning the individual or to object to processing as well as the right to data portability and the right to withdraw consent as the case may be (as further described in Section C of this Controller Policy);
- the right to lodge a complaint with the Commission, without exhausting BMC's complaints process;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- the categories of Personal Information processed.

BMC will provide such information to the individual at the time when the Personal Information is obtained by BMC, or at any other time specified by UK Applicable Law, unless:

- the individual already has such information;
- the provision of such information proves impossible or would involve a disproportionate effort;
- obtaining or disclosure is expressly laid down by a rule of domestic law and which provides appropriate measures to protect the individual's legitimate interests;
- where the Personal Information must remain confidential subject to an obligation of professional secrecy regulated by a rule of domestic law, including a statutory obligation of secrecy.

Rule 2B – BMC will only obtain and process Personal Information for those purposes which are known to the individual or which are compatible with such purposes ("Purpose limitation").

Rule 1A provides that BMC will comply with any applicable legislation relating to the collection of Personal Information. This means that where BMC collects Personal Information subject to UK GDPR, BMC may only collect and process it for specific, explicit and legitimate purposes, and not process that Personal Information in a way which is incompatible with those purposes.

Under Rule 2B, BMC will identify and make known the purposes for which Personal Information will be processed (including the secondary processing and disclosures of the information), prior to such processing, unless there is a legitimate basis for not doing so, as described in Rule 2A. In particular, if BMC collects Personal Information for a specific purpose and subsequently BMC wishes to process the information for a different or new purpose, the relevant individuals will be made aware of such a change prior to that further processing unless:

- it is compatible with the initial purposes agreed with the individual; or
- there is a legitimate basis for not doing so consistent with UK Applicable Law.

In certain cases, for example, where there is processing of Sensitive Personal Information, or where BMC is not satisfied that the processing is compatible with the initial purposes agreed with the individual, the individual's consent to the new processing or disclosures may be necessary.

Rule 2C – BMC will process Personal Information lawfully ("Lawfulness")

In accordance with UK Data Protection Law, any processing of Personal Information by BMC shall be based on one of the following legal grounds:

(a) the individual has given consent to the processing of his Personal Information for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which BMC is subject; or

(d) processing is necessary for the purposes of the legitimate interests pursued by BMC or by a third party, where such interests are not overridden by the interests or fundamental rights and freedoms of the individuals.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – BMC will keep Personal Information accurate and up to date ("Accuracy").

In order to ensure that the Personal Information held by BMC is accurate and up to date, BMC actively encourages individuals to inform BMC when their Personal Information changes.

Rule 3B – BMC will only process Personal Information for as long as is necessary for the purposes for which it is collected and further processed ("Storage limitation").

BMC will comply wi'h BMC's record retention policies and procedures as revised and updated from time to time.

Rule 3C – BMC will only process Personal Information which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("Data minimisation").

BMC will identify the minimum amount of Personal Information necessary in order to properly fulfil its purposes.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES AND NOTIFYING DATA BREACHES

Rule 4A – BMC will adhere to its security and breach notification policies.

BMC will implement appropriate technical and organizational measures to protect Personal Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information, in particular where processing involves transmission of Personal Information over a network, and against all other unlawful forms of processing.

To this end, BMC will comply with the requirements in the security policies in place within BMC as revised and updated from time to time together with any other security procedures relevant to a business area or function.

BMC will implement and comply with breach notification policies as required by UK Data Protection Law:

- Notification to the Commission: BMC shall without undue delay and, in any case, no later than 72 hours after having become aware of it, notify the Personal Information breach to the Commission, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Commission is not made within 72 hours, it shall be accompanied by reasons for the delay.

- Communication to the individual: When the breach is likely to result in a high risk to the rights and freedoms of the individuals, BMC shall communicate the breach to such individuals without undue delay.

BMC will additionally notify without undue delay any data breaches to the responsible BCR Group Member established in the UK and the other relevant privacy officer/function.

Pursuant to Articles 33 and 34 of UK GDPR, personal data breaches are documented (including the facts relating to the personal data breach, its effects and the remedial action taken). Such documentation is available to the Commission on request.

Rule 4B – BMC will ensure that providers of services to BMC also adopt appropriate and equivalent security measures.

Pursuant to Article 28.3 of UK GDPR, providers of a service acting as data processors to any of the BMC entities, having access to the Personal Information of past, current and potential employees (including contractors and contingent workers), customers, resellers, suppliers, service providers and other third parties, are required to enter into strict contractual obligations evidenced in writing, dealing with the security of that information, to ensure that such service providers act only on BMC's instructions when using that information, and that they have in place appropriate technical and organizational security measures to safeguard Personal Information.

Contracts with such providers of service will include in particular:

- a requirement to process Personal Information based solely on BMC's instructions, unless processing is required by UK Applicable Law;
- the rights and obligations of BMC;
- the scope of processing (duration, nature, purpose and the categories of Personal Information);
- an obligation for the provider to:
  - implement appropriate technical and organizational measures to protect the Personal Information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access;
  - notify BMC without undue delay after becoming aware of a personal data breach and provide full cooperation and assistance to BMC to enable BMC to comply with its obligations under Rule 4A;
  - provide full cooperation and assistance to BMC to allow individuals to exercise their rights under the Controller Policy;
  - provide full cooperation to BMC so it 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 the request of BMC, 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 BMC and the provider or with BMC's written consent.

RULE 5 – HONORING INDIVIDUALS' RIGHTS

This Rule 5 is without prejudice of the rights given to individuals to enforce this Controller Policy as third party beneficiaries, as per Section C of this Controller Policy.

Rule 5A – BMC will adhere to the Individuals' Rights Requests Procedure and respond to any queries or requests made by individuals in connection with their Personal Information, in accordance with UK Applicable Law.

Individuals are entitled to obtain from BMC confirmation as to whether or not their Personal Information are being processed and, where that is the case, be supplied with a copy of Personal Information held about them (including information held in both electronic and paper records). This is known as the "right of access" in UK Data Protection Law. BMC will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) when dealing with requests from individuals for access to their Personal Information.

Rule 5B – BMC will deal with individual rights in accordance with the Individuals' Rights Requests

Procedure.

Individuals are entitled, in accordance with UK Applicable Law, to request access, rectification or erasure of their Personal Information and, in certain circumstances, to object to or restrict the processing of their Personal Information. Individuals may also exercise their right to portability. BMC will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSFERS TO THIRD PARTIES OUTSIDE THE UK

Rule 6A – BMC will not transfer Personal Information to third parties outside the UK without ensuring adequate protection for the transferred Personal Information in accordance with UK GDPR.

Transfers of Personal Information to third parties outside the BMC Group Members are not allowed without having in place an appropriate safeguard as described in Articles 45, 46, 47 or 49 of UK GDPR. In particular, such appropriate safeguard will be required to cover onward transfers of transferred data.

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7A – BMC will only process Sensitive Personal Information if it is absolutely necessary to process it.

Sensitive Personal Information includes information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation, as well as Personal Information relating to criminal convictions and offences.

BMC will assess whether Sensitive Personal Information is required for the proposed processing and whether it is absolutely necessary in the context of its business. Such Sensitive Personal Information will be processed in accordance with relevant provisions of UK GDPR, including articles 6, 9 and 10 of UK GDPR.

Rule 7B – BMC will only process Sensitive Personal Information where the individual's explicit consent has been obtained unless BMC has an alternative legitimate basis for doing so consistent with UK Applicable Law.

In principle, individuals must explicitly agree to BMC collecting and using Sensitive Personal Information unless BMC is required to do so by UK Applicable Law or processing is for the purposes expressly authorized by UK Applicable Law.

Individual permission to process Sensitive Personal Information must be specific, informed, unambiguous and freely given. BMC may also rely on other lawful basis to process Sensitive Personal Information, in accordance with article 9 of UK GDPR and as described in Appendix 8.

Personal Information relating to criminal convictions and offences shall only be processed when authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects.

RULE 8 – LEGITIMIZING DIRECT MARKETING

Rule 8 – BMC will allow customers to opt out of receiving marketing information.

All individuals have the data protection right to object, at any time and free of charge, to the processing of their Personal Information for direct marketing purposes, including profiling to the extent that it is related to such direct marketing, and BMC will honor all such opt out requests and no longer process the Personal Information for this purpose.

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Where decisions regarding individuals are made solely by automated means, individuals will have the right to know the existence of the automated decision-making process and the logic involved in the decision. BMC will take necessary measures to protect the rights, freedoms and legitimate interests of individuals.

There are particular requirements in place under UK Data Protection Law to ensure that no evaluation of, or decision about, an individual which produces legal effects concerning him or her, or significantly affects him or her, can be based solely on the automated processing of Personal Information, unless there is a legal basis for such decision under UK Applicable Law, and measures are taken to protect the rights, freedoms and legitimate interests of individuals.

Individuals shall have the right to object to a decision solely based on automated decision-making, in accordance with UK Applicable Law, and shall at least have the right to obtain human intervention on the part of BMC, to express their point of view and to contest the decision.

SECTION B: PRACTICAL COMMITMENTS

RULE 10 – COMPLIANCE

Rule 10 – 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 Controller 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 Controller Policy on a day-to-day basis. A summary of the roles and responsibilities ’f BMC's privacy team is set out in Appendix 2.

RULE 11 – TRAINING

Rule 11 – 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 attached as Appendix 3.

RULE 12 – AUDIT

Rule 12 – BMC will comply with the Controller Data Protection Binding Corporate Rules Audit Protocol set out in Appendix 4.

RULE 13 – COMPLAINT HANDLING

Rule 13 – BMC will comply with the Controller Data Protection Binding Corporate Rules Complaint Handling Procedure set out in Appendix 5.

RULE 14 – COOPERATION WITH THE COMMISSION

Rule 14 – BMC will comply with the Controller Data Protection Binding Corporate Rules Cooperation Procedure set out in Appendix 6.

RULE 15 – UPDATE OF THE CONTROLLER POLICY

Rule 15 – BMC will comply with the Controller Data Protection Binding Corporate Rules Updating Procedure set out in Appendix 7.

RULE 16 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE CONTROLLER POLICY

Rule 16A – BMC will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Controller Policy or such legislation has a substantial effect on its ability to comply with the Controller 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 that has not been recognized by the UK as ensuring an adequate level of protection, 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 reasons 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 a third country or a measure indicating an application of such laws in practice that is not in line with the requirements in this Policy, BMC will promptly inform:

(a) The Group Member acting as the controller in the UK;

(b) 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 Controller Policy, BMC shall promptly identify supplementary 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 Commission to do so.

Rule 16B – BMC will take appropriate action if (i) it receives a legally binding request for the disclosure of Personal Information transferred pursuant to this Controller 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 Controller Policy in accordance with the laws of a third country.

4. 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, it will promptly notify the Commission.

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.

If in specific cases the suspension and/or notification to the Commission is prohibited under the laws of the third country, BMC will use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. BMC will document its best efforts in order to be able to demonstrate them.

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.).

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.

5. 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 Group Member established in the UK. 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 the following elements of this Controller Policy as third party beneficiaries:

- data protection principles (Rules 2A, 2B, 2C, 3A, 3B, 3C, 4A, 4B, 6 and 7 of Part II of this Controller Policy);
- transparency and easy access to the Controller Policy (Section C of Part II of this Controller Policy);
- rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing (Rules 5A, 5B, 8 and 9 of Part II and Appendix 1 of this Controller Policy);
- national legislation preventing respect of the Controller Policy (Rule 16 of Part II of this Controller Policy);
- right to complain (Rule 13 of Part II and Appendix 5 of this Controller Policy);
- cooperation duties with the Commission (Rule 14 of Part II of this Controller Policy and Appendix 6); and
- liability and jurisdiction provisions (Section C of Part II of this Controller Policy).

Third party beneficiary rights are without prejudice of the UK Individual rights provided by UK GDPR, to request access, rectification or erasure of Personal Information, to object to or restrict the processing of Personal Information, and to data portability, as described in Rule 5 of this Controller Policy.

This Section C applies where UK Individual's Personal Information is protected under UK Data Protection Laws. This is the case when:

- the UK Individuals' Personal Information are processed in the context of the activities of BMC Software Ltd ("UK Group Member");
- a non-UK Group Member (or its third party processor offers goods and services to UK Individuals in the UK; or
- a non-UK Group Member monitors the behaviour of those UK Individuals as far as their behaviour takes place in the UK,
- and that Group Member then transfers those UK Individuals' Personal Information to a non-UK Group Member for processing under this Controller Policy.

It is agreed that such third party beneficiary rights shall not be open to UK Individuals whose Personal Information is not handled by BMC or on BMC's behalf.

Should a Group Member breach one of such enforceable elements, the UK Individual defined hereabove

who benefits from this third party beneficiary right shall be 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.

(b) *Complaints to the Commission*: UK Individuals may lodge a complaint to the Commission.

(c) *Jurisdiction*: UK Individuals may bring proceedings against BMC before the UK competent courts.

(d) *Liability*: UK Individuals may seek appropriate redress from the UK Group Member including the judicial remedy of any breach of the enforceable elements listed in this section C by any provider of a service, acting as a processor, and/or by any non-UK Group Members, and, where appropriate receive compensation from the UK Group Member for any damage suffered as a result of a breach of the enforceable elements listed in this section C. For the sake of clarity, UK Individuals shall not be required to go through judicial processes or to sign settlement or non-disclosures agreements, in order to seek redress or compensation.

(e) It is agreed that should the Group Member be located outside the UK, BMC Software Ltd shall accept responsibility for and agree to take the necessary action to remedy the acts of such Group Member and to pay compensation for any material or non-material damages resulting from a violation of the enforceable elements listed in this section C by such Group Member. The UK Group Member will accept liability as if the violation had taken place by him in the UK instead of the Group Member established outside the UK.

(f) *Transparency and Easy Access to the Controller Policy*: UK Individuals benefiting from third party beneficiary rights shall be provided with an access to this Controller Policy in full on www.bmc.com.

(g) *Burden of Proof*: In the event of a claim being made in which a UK Individual has suffered damage where that UK Individual can demonstrate that it is likely that the damage has occurred because of a breach of the Controller Policy by a Group Member located outside the UK, BMC has agreed that the burden of proof to show that the Group Member located outside the UK is not responsible for the breach, or that no such breach took place, will rest with BMC Software Ltd. If BMC Software Ltd can prove that the Group Member established outside the UK is not responsible for the event giving rise to the damage, BMC Software Ltd may discharge itself from any responsibility.

PART III: APPENDICES

APPEN–IX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE

1. Introduction

1.1 When BMC collects, processes or transfers Personal Information for BMC's own purposes, BMC is deemed to be a *controller* of that information and is therefore primarily responsible for demonstrating compliance of processing with the requirements of applicable data protection law.

1.2 When BMC acts as a controller, individuals subject to UK Data Protection Laws have the following rights, which will be dealt with in accordance with the terms of this Individuals' Rights Requests Procedure ("**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.

1.3 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.

1.4 This Procedure explains how BMC deals with an individual's rights request relating to Personal Information ("**Request**") provided it falls into the categories stated in section 1.2 above.

1.5 Where a Request is subject to UK Data Protection Law, such Request will be dealt with by BMC in accordance with this Procedure. Where the Request is subject to third country national legislation, BMC may give precedence to applicable third country national legislation over the Controller Policy, in accordance with Rule 1A of the Controller Policy.

1.6 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.

2. General Process

2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 BMC must respond to Requests without undue delay and in any event within one month (or any shorter period as may be stipulated under local law) of receipt of the Request. That period may be extended by two further months where necessary, taking into account the complexity and number of the Requests, in which case the individual will be informed accordingly.

2.6 The Group Data Protection Officer will contact the individual in writing to acknowledge receipt of the Request and, if required, seek confirmation of identity or ask for further information.

2.7 The Group Data Protection Officer may decline the Request if one of the below exemptions applies:

- The Request is manifestly unfounded or excessive; or
- The execution of the Request would adversely affect the rights and freedoms of others; or
- The Personal Information is not subject to UK Data Protection Laws and the execution of the Request would require disproportionate effort.

2.8 The Group Data Protection Officer will assess each Request individually to determine whether any of the above-mentioned exemptions applies.

2.9 The execution of Requests will be provided free of charge. However, in case or Requests manifestly unfounded or excessive, BMC may either charge a reasonable fee or refuse to act on the Request.

2.10 All queries relating to this Procedure are to be addressed to the Group Data Protection Officer via privacy@bmc.com.

3. Right of Access

3.1 Individuals are entitled to obtain:

- confirmation as to whether or not Personal Information relating to them are being processed and, where that is the case;
- access to the Personal Information processed by BMC 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 UK Data Protection Law 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, where such Personal Information was not 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;

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

(ii) 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;

(iii) Personal Information has been unlawfully processed;

(iv) Personal Information must be erased for compliance with a legal obligation in UK Applicable Law to

which BMC is subject; or

(v) 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:

(ii) the accuracy of Personal Information is contested by the individual concerned, for a period enabling BMC to verify its accuracy;

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

(iv) BMC 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

(v) the individual has objected to processing pending the verification whether the legitimate grounds of BMC 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.

7.4 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 BMC, or BMC legitimate interests, unless BMC 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; or

(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 BMC 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 Sensitive 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 Controller 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 Controller Policy, including:

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

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

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

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

(v) Reviewing investigations and compliance monitoring of the Controller Policy, as reported by the Core Privacy Team.

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

(vii) Facilitating communications on the Controller 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 Controller Policy, as described in the Controller Data Protection Binding Corporate Rules of BMC Software Audit Protocol ("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 Controller Policy at all levels in their organizations.

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

(iii) Ensuring that BMC's business objectives align with the Controller 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 Controller 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 Controller Policy and BMC's privacy initiatives including:

(i) Responding to inquiries and complaints relating to the Controller 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 Controller 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 Controller 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

Controller Policy and BMC's related policies and business practices.

(v) Promoting the Controller 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 Controller 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 Controller Policy and on data protection legal requirements in accordance with the requirements of the Controller Data Protection Binding Corporate Rules of BMC Software Privacy Training Requirements.

(x) Escalating issues relating to the Controller 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 Controller Policy as set out in the Controller 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 Controller 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 Controller Policy in their jurisdiction.

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

(iii) Oversee handling of local complaints from data subjects.

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

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS

1. Background

1.1 The Controller Policy provides a framework for the transfer of Personal Information between BMC 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 Controller Polic'.

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 'f BMC's formal privacy online training modules. Training on the Controller Policy is overseen 'y 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 Controller 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 Controller 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 Controller 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 Controller 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 Controller 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 Controller Policy

4.1 BMC's training on the Controller 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 Controller Policy

(d) Terminology and concepts

4.1.2 The Controller Policy:

(a) An explanation of the Controller Policy

(b) Practical examples

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

4.1.3 Where relevant to an employee's role, training will cover the following procedures under the Controller 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 Controller 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 Controller Policy is to safeguard Personal Information transferred between the BMC Group Members.

1.2 The Controller Policy requires approval from the Commission. One of the requirements of the Commission is that BMC audits compliance with the Controller 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 Controller 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 Controller Policy as required by the Commission, this is only one way in which BMC ensures that the provisions of the Controller Policy are observed and corrective actions taken as required.

2. Approach

2.1 Overview of audit

2.1.1 Compliance with the Controller 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 Controller Policy and will ensure that such audits address all aspects of the Controller Policy, including mechanisms to ensure any corrective actions are implemented within a reasonable time in accordance with the BMC Audit Protocol. 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.

2.1.3 To the extent that BMC acts as a controller, audits of compliance with the commitments made in Part II of the Controller Policy may also be extended to any processor acting on BMC's behalf in respect of such processing.

2.2 Timing and scope of audit

2.2.1 Audit of the Controller Policy will take place:

(a) at least **annually** in accordance with BMC's **corporate audit program**; and/or

(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 The scope of the audit performed 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. Audits will cover all aspects of the Controller Policy, including applications, IT systems, databases that process Personal Information, onward transfers, decisions taken as regards mandatory requirement under national laws that conflicts with the BCRs, review of the contractual terms used for the transfers out of the Group (to Controllers or Processors of data).

2.3 Auditors

2.3.1 Audit of the Controller 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 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.

2.3.3 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.

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

2.4 Report

BMC's **Assurance Department** will provide the results of any audit of the Controller 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.

2.4.1 Upon request, BMC shall provide copies of the results of any audit of the Controller Policy to the Commission.

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE

1. Introduction

1.1 The Controller 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 Controller Policy are dealt with.

2. How UK Individuals can bring complaints

2.1 UK Individuals who are third party beneficiaries of this Controller Policy can bring complaints against any Group Member in writing by contacting BMC's Group Data Protection Officer at the details provided on page 5 of the Controller Policy or by emailing privacy@bmc.com. These are the contact details for all complaints made under the Controller 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 BMC's Group Data Protection Officer will handle all complaints arising under the Controller Policy where a complaint is brought in respect of the collection and processing of Personal Information where BMC is the controller of that information. BMC's Group Data Protection Officer will liaise with its colleagues from the relevant business and support units as appropriate to deal with the complaint.

4. What is the response time?

4.1 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.

4.2 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).

5. When a complainant disputes a finding

5.1 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.

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

5.3 If the matter relates to Personal Information which has been exported to a Group Member outside the UK and a UK Individual wants to make a claim against BMC, the claim may be made against the UK Group Member responsible for exporting the Personal Information.

APPENDIX 6 - COOPERATION PROCEDURE

1. Introduction

1.1 This Cooperation Procedure sets out the way in which BMC will cooperate with the Commission in relation to the Controller Policy.

2. Cooperation Procedure

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

2.2 BMC will actively review and consider:

2.2.1 any decision made by the Commission on any data protection law issues that may affect the Controller Policy; and

2.2.2 any guidance published by the Commission in connection with BCRs for controllers.

2.3 BMC will provide copies of the results of any audit of the Controller Policy and data protection impact assessment to the Commission upon the Commission's request.

2.4 BMC agrees that:

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

2.4.2 The Commission may audit Group Members located outside the UK for the purpose of reviewing compliance with the Controller Policy in accordance with UK Applicable Law.

2.5 BMC agrees to consider any communication or recommendations from the Commission and abide by a formal decision or notice of the Commission on any issues relating to the interpretation and application of the Controller Policy. 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 Controller Policy to the Commission, individuals and to the BMC Group Members bound by the Controller Policy.

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

1.4 No transfer is made to a new Group Member until the new Group Member is effectively bound by the

Controller Policy and can deliver compliance.

2. Material changes to the Controller Policy

2.1 BMC will promptly communicate any material changes to the Controller 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 Controller Policy, or affect the binding nature of the Controller Policy) to the Commission and all Group Members. Material changes will be communicated to the Commission at least once a year.

3. Administrative changes to the Controller Policy

3.1 BMC will communicate changes to the Controller Policy which are administrative in nature (including changes in the list of Group Members) to the Group Members regularly and to 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 Controller Policy.

4. Communicating and logging changes to the Controller Policy

4.1 The Controller Policy contains a change log which sets out the date of revisions to the Controller 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 Controller Policy.

4.2 BMC will communicate all changes to the Controller Policy, whether administrative or material in nature, to the Group Members which shall be automatically bound by such changes; and

4.3 BMC's Group Data Protection Officer will maintain an up to date list of the changes made to the list of Group Members bound by the Controller Policy. This information will be available on request from BMC.

5. New Group Members

5.1 BMC's Group Data Protection Officer will ensure that no transfer to a new Group Member is made under the Controller Policy until that new Group Member is effectively bound by the Policy and can deliver compliance.

APPENDIX 8 - MATERIAL SCOPE OF THE CONTROLLER POLICY

1. Introduction

1.1 BMC's Controller 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 Controller 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 BMC's business structure as well as the allocation of roles and responsibilities are set in such a manner that the company can operate 24/7, according to BMC's "follow the sun" model. As a consequence of that distributed model, Personal Information processing activities are broadly shared between BMC countries and regions.

2. 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.*

3. 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.*

4. 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.*

5. 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	Anyspace, Hämeentie 135 A, 00560, Finland		
France	BMC Software France SAS	313400681	Cœur Défense, 100, Esplanade du Général de Gaulle, 10th Floor Tower A, 92400 Courbevoie, France		
Germany	BMC Software GmbH	HRB 24281	Wiesenhüttenstr. 11,60329 Frankfurt am Main, Germany		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Greece	BMC Software Hellas MEPE	9300937852	1 Alamanas & Delfon, 15125 Marousi, Greece	Privacy@bmc.com	Categories of data listed in Appendix 8
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		
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		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Sweden	BMC Software AB	556207-5795	Vasagatan 38, Stockholm, SE- 111 20, Sweden	Privacy@bmc.com	Categories of data listed in Appendix 8.
Switzerland	BMC Software GmbH	CH-020.4.002.762-1	Talstrasse 83, 8001 Zürich, Switzerland		
The Netherlands	BMC Software Distribution B.V.	30106755	Boeingavenue 220, 1119PN Schiphol-Rijk, The Netherlands		
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 Street, Sydney, NSW 2000, Australia		
Brazil	BMC Software do Brasil Ltda.	00.723.020/0001-90	Avenida Rebouças, 3970 e Avenida Dra. Ruth Cardoso, 8501, 22º andar, Sala 2, Eldorado Business Tower, Pinheiros, Zip Code 05402-918, Brazil		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Canada	BMC Software Canada Inc.	1654693	150 King Street West, Suite 306-02, Toronto, Ontario, Canada	Privacy@bmc.com	Categories of data listed in Appendix 8.
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		
Dubai	BMC Software Limited - Dubai Branch	505326	U-Bora Commercial Tower, Building No.2, Business Bay, 40th Floor, Unit 4003, Dubai, United Arab Emirates		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Hong Kong	BMC Software (Hong Kong) Limited	543682	Level 23, One Island East, No.18 Westlands Road, Taikoo Place, Quarry Bay, Hong Kong	Privacy@bmc.com	Categories of data listed in Appendix 8.
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, 24F1-32-2 Honcho, Nakano-ku , Tokyo, 164-8721		
Korea	BMC Software Korea, Ltd.	110111-1285877	9 FL Two IFC, 10 Gukjekeumyung-ro, Youngdeungpogu, Seoul 07326, South Korea		
Malaysia	BMC Software Asia Sdn Bhd	199901024358	Level 15, 1 First Avenue 2A Dataran Bandar Utama Damansara, 47800 Petaling Jaya, Malaysia		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
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	Privacy@bmc.com	Categories of data listed in Appendix 8.
	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		
New Zealand	BMC Software (New Zealand) Limited	28 009 503	Level 2, 40 Lady Elizabeth Lane Wellington, 6011, New Zealand		
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		

Country	Group Member name	Registration number	Registered Office address	Contact email (common)	Expected categories of data transferred (common)
Singapore	BMC Software Asia Pacific Pte. Ltd.	199504342D	600 North Bridge Road, #20-01/10 Parkview Square, 188778, Singapore	Privacy@bmc.com	Categories of data listed in Appendix 8.
Taiwan	Tawain Representative Office of BMC Software (Hong Kong) Limited	28986710	11/F, 1172/1173, No.1, Songzhi Rd., Taipei, 11047, Taiwan		
Thailand	BMC Software (Thailand) Limited	(3)82/2543	63 Wireless Road Level 23, Athenee Tower Pathumwan, Lumpini, Bangkok, 10330, Thailand		
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.

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