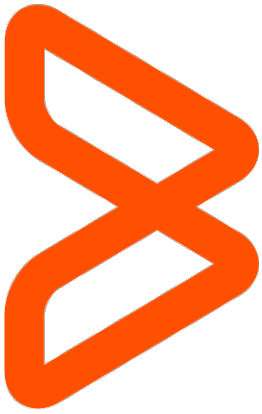

# EU Controller and Processor Data Protection Binding Corporate Rules of BMC Software

bmc

# TABLE OF CONTENTS


TABLE OF CONTENTS 1

INTRODUCTION 2

PART I: BACKGROUND AND ACTIONS 3

WHAT IS DATA PROTECTION LAW? 3

HOW DOES 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 14

SECTION C: THIRD-PARTY BENEFICIARY RIGHTS 20

PART III: BMC AS A PROCESSOR 22

SECTION A: BASIC PRINCIPLES 23

SECTION B: PRACTICAL COMMITMENTS 28

SECTION C: THIRD-PARTY BENEFICIARY RIGHTS 33

PART IV: APPENDICES 36

APPENDIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE 36

APPENDIX 2 - COMPLIANCE STRUCTURE 42

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS 46

APPENDIX 4 - AUDIT PROTOCOL 49

APPENDIX 5 - COMPLAINT HANDLING PROCEDURE 52

APPENDIX 6 - COOPERATION PROCEDURE 54

APPENDIX 7 - UPDATING PROCEDURE 55

APPENDIX 8 – MATERIAL SCOPE 57

APPENDIX 9 – LIST OF BCR GROUP MEMBERS 69

APPENDIX 10 – LIST OF DEFINITIONS 74

DOCUMENT INFORMATION 76

# INTRODUCTION

These Controller and Processor Data Protection Binding Corporate Rules of BMC Software (the “**Policy**”) establish BMC Software's ("**BMC**") approach to compliance with European data protection law including transfers of personal information between BMC group members ("**Group Members**") (a list of which is available at www.bmc.com).

For the purposes of this Policy,BMC is defined as all BMC Software entities bound by the Policy as Group Members.BMC entities bound by the Policy as Group Members are listed in Appendix 9.

BMC must comply with and respect the Policy when collecting and using personal information. In particular, the Policy describes the standards that Group Members must apply when they transfer personal information internationally to other Group Members, whether Group Members are transferring personal information for their own purposes or when providing services to a third-party controller.

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 Policy applies to all personal information of past, current and potential employees, customers, resellers, suppliers, service providers and other third parties wherever it is collected and used in conjunction with BMC business activities and the administration of employment. Additional details about the material scope of the Controller policy are set out in Appendix 8.

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

The Policy is published in full on BMC’s website accessible at www.bmc.com and on BMC’s employee intranet.

# PART I: BACKGROUND AND ACTIONS

## WHAT IS DATA PROTECTION LAW?

European[1] data protection law gives people certain rights in connection with the way in which their "**personal information**"[2] is used. If organizations do not comply with data protection law, they may be subject to sanctions and penalties imposed by data protection authorities and the courts. When Group Members collect and use the personal information of their 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 data protection law.

Under data protection law, when an organization collects, uses 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. The Policy describes how BMC will comply with data protection law in respect of processing undertaken in its capacity as both a controller and as a processor.

## HOW DOES DATA PROTECTION LAW AFFECT BMC INTERNATIONALLY?

European data protection law prohibits the transfer of personal information to countries outside Europe that do not ensure an adequate level of data protection. Some of the countries in which BMC operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

## WHAT IS BMC DOING ABOUT IT?

Group Members must take proper steps to ensure that they use personal information on an international basis in a safe and lawful manner. The purpose of the Policy, therefore, is to set out a framework to satisfy the standards contained in European data protection law and, as a result, provide an adequate level of protection for all personal information used and collected in Europe and transferred from Group Members within Europe to Group Members outside Europe.

Group Members will apply the Policy globally, and in **all cases** where Group Members process personal information both manually and by automatic means, when the personal information

[1] For the purpose of this Policy, reference to Europe means the European Economic Area or "EEA" (namely the EU Member States plus Norway, Iceland and Liechtenstein) plus Switzerland.

[2] "Personal information" means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR"), available at http://eur-lex.europa.eu/.

relates to past, current and potential employees, customers, resellers, suppliers, service providers and other third parties.

The Policy applies to all Group Members and their employees worldwide and requires that:

- Group Members who collect, use or transfer personal information as a controller must comply with **Part II** of the Policy together with the practical procedures set out in the appendices in **Part IV** of the Policy; and

- Group Members who collect, use or transfer personal information to provide services to a third party as a processor or who provide a service to other Group Members in their capacity as a processor must comply with **Part III** of the Policy together with the practical procedures set out in the appendices in **Part IV** of the Policy. Some Group Members may act as both a controller and a processor and must therefore comply with Parts II, III and IV of the Policy as appropriate.

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

## FURTHER INFORMATION

If you have any questions regarding the provisions of the Policy, your rights under the 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.

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

The Group Data Protection Officer is responsible for monitoring compliance with the Policy and ensuring that changes to the Policy are notified, to the Group Members, to the clients, to the Supervisory Authorities and to individuals whose personal information is processed by BMC, as required by applicable law. If you are unhappy about the way in which BMC has used your personal information, BMC has a separate complaint handling procedure which is set out in Part IV, Appendix 5.

# PART II: BMC AS A CONTROLLER

Part II of the Policy applies in all cases where a Group Member collects, uses and transfers personal information as a controller.

Part II of the Policy is divided into three sections:

- **Section A**: addresses the basic principles of European data protection law that a Group Member must observe when it collects, uses and transfers personal information as a controller.
- **Section B**: deals with the practical commitments made by BMC to the Supervisory Authorities in connection with the Policy.
- **Section C**: describes the third-party beneficiary rights that BMC has granted to individuals under Part II of the Policy.

## SECTION A: BASIC PRINCIPLES

### RULE 1 – COMPLIANCE WITH LOCAL LAW AND ACCOUNTABILITY

**Rule 1A – BMC will first and foremost comply with local law where it exists.**

As an organization, BMC will comply with any applicable legislation relating to personal information, and will ensure that where personal information is collected and used, 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 Policy, BMC's position will be to process personal information adhering to the 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 Part II of the Policy.

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

BMC will maintain a record of processing activities carried under its responsibility in accordance with applicable law. This record shall be maintained in writing, including in an electronic form, and shall be made available to the competent Supervisory Authority upon request.

The record shall contain:

- the name and contact details of the Group Member acting as the controller and, where applicable, the joint controller, and the data protection officer;
- the purposes of the processing;

- a description of the categories of individuals and of the categories of personal information;

- the categories of recipients to whom the personal information have been or will be disclosed including recipients in third countries or international organizations;

- where applicable, transfers of personal information to a third country or an international organization, including the identification of that third country or international organization;

- where possible, the envisaged time limits for erasure of the different categories of personal information;

- where possible, a general description of the technical and organizational security measures applicable to processing.

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. 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 competent Supervisory Authority, prior to processing.

Appropriate technical and organizational measures will be implemented which are designed to make data protection principles effective and to facilitate compliance with the requirements set up by this 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.

Every entity acting as a controller shall be responsible for and be able to demonstrate compliance with this Policy.

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

### Rule 2A – BMC will explain to individuals how that information will be used ("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 used. 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, and includes the following:

- the identity and contact details of the BMC Group Member acting as a controller,
- the contact details of the Group Data Protection Officer;
- the purposes for which personal information will be processed;
- the legal basis for processing that data;
- who personal information will be shared with;
- countries outside of Europe where 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 or to object to processing as well as the right to data portability and the right to withdraw consent as the case may be;
- the right to lodge a complaint with a Supervisory Authority;
- 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 individual;
- whether the provision of personal information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether individuals are obliged to provide personal information and of the possible consequences of failure to provide such information;
- 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 applicable law, unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, legal proceedings, or where otherwise permitted by law) or unless the individual already has such information.

**Rule 2B – BMC will only obtain and use 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 in Europe and local law requires that BMC may only collect and use it for specific, explicit and legitimate

purposes, and not use that personal information in a way which is incompatible with those purposes, BMC will honor these obligations.

Under Rule 2B, BMC will identify and make known the purposes for which personal information will be used (including the secondary uses 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 use 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 the applicable law of the European country in which the personal information was collected.

In certain cases, for example, where the processing is 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 uses or disclosures may be necessary.

**Rule 2C – BMC will process personal information lawfully ("Lawfulness")**

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; or

(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; or

(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; or

(e) any other legal ground provided by applicable Union or Member state law.

## 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 keep personal information for as long as is necessary for the purposes for which it is collected and further processed ("Storage limitation").**

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

**Rule 3C – BMC will only keep personal information which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("Data minimization").**

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 applicable data protection law:

- Notification between Group Members: any Group Member becoming aware of a personal information breach shall without undue delay notify the Group Member acting as an exporter and the Group Data Protection Officer. When the Group Member becoming aware of the breach was acting as a processor on behalf of another Group Member, acting as a controller and who was not the data exporter, the Group Member acting as a processor will also notify that Group Member acting as a controller;

- Notification to the Supervisory Authority: BMC shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal information breach to the competent Supervisory Authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay;

- Notification to individuals: 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.

Personal information breaches shall be documented in accordance with applicable law (including the facts relating to the breach, its consequences and the remedial action taken). Such documentation will be made available to the competent Supervisory Authority upon request.

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

European law expressly requires that where a provider of a service (acting as a processor) to any of the BMC entities has 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, strict contractual obligations evidenced in writing dealing with the security of that information are imposed consistent with the applicable law of the European country in which the personal information was collected, to ensure that such service providers act only on BMC's instructions when using that information (unless such service provider is required to do so by applicable law), and that they have in place appropriate technical and organizational security measures to safeguard personal information. Whenever the provider of a service is not a Group Member, BMC will do its best efforts to ensure that such provider of service has committed in writing to comply with obligations consistent with this Policy.

Contracts with such providers of service will set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal information and categories of individuals and the obligations and rights of the BMC. Such contracts shall stipulate, in particular, that the provider:

- processes the personal information only on documented instructions from BMC, including with regard to transfers of personal information to a third country or an international organization, unless required to do so by Union or Member State law to which the provider is subject; in such a case, the provider shall inform BMC of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- ensures that persons authorized to process the personal information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk;

- shall not engage another processor without prior specific or general written authorization of BMC. In the case of general written authorization, the provider shall inform BMC of any intended changes concerning the addition or replacement of other processors, thereby giving BMC the opportunity to object to such changes. Where a provider engages another processor for carrying out specific processing activities on behalf of BMC, the same data protection obligations as set out in the contract or other legal act between BMC and the provider shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures. Where that other processor fails to fulfil its data protection obligations, the provider shall remain fully liable to BMC for the performance of that other processor's obligations;

- taking into account the nature of the processing, assists BMC by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of BMC's obligation to respond to requests for exercising the data subject's rights laid down in GDPR;

- assists BMC in ensuring compliance with its obligations to ensure security of processing, notify personal information breaches, carry out data protection assessments and consult the supervisory authority, taking into account the nature of processing and the information available to the processor;

- at the choice of BMC, deletes or returns all the personal information to BMC after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal information;

- makes available to BMC all information necessary to demonstrate compliance with the obligations laid down in GDPR and allow for and contribute to audits, including inspections, conducted by BMC or another auditor mandated by BMC. The provider shall immediately inform BMC if, in its opinion, an instruction infringes GDPR or other Union or Member State data protection provisions.

## RULE 5 – HONORING INDIVIDUALS' RIGHTS

**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 applicable law.**

Individuals are entitled (by making a written request to BMC where required) to obtain from BMC confirmation as to whether or not their personal information is 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 European 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 applicable law, to request 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. Any rectification or erasure of personal information or restriction of processing requested by an individual will be communicated to recipients to whom personal information has been disclosed, unless it proves impossible or involves disproportionate effort. BMC will inform that individual about such recipients upon request. BMC will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) in such circumstances.

**Rule 5C – 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 European 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, and measures are taken to protect the rights, freedoms and legitimate interests of individuals.

Individuals 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. BMC will follow the steps set out in the Individuals' Rights Requests Procedure (see Appendix 1) in such circumstances

**Rule 5D – 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 use 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. 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 OF PERSONAL INFORMATION OUTSIDE EUROPE

**Rule 6 – BMC will not transfer personal information to third parties outside Europe without ensuring adequate protection for the information in accordance with the standards set out by the Policy.**

We must comply with any restrictions under applicable data protection laws which prohibit the transfers of personal information to third countries unless appropriate steps are taken to ensure the transferred data continues to remain protected to the standard required in the country or region from which it is transferred.

Whenever transferring personal information outside Europe, we must implement appropriate safeguards, such as contractual clauses so as to guarantee the level of protection of the personal information that is being transferred outside Europe.

We will take appropriate action in case national legislation in a third country outside Europe prevents compliance with this Policy, in accordance with Rule 14.

## RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

**Rule 7A – BMC will only transfer and use sensitive personal information if it is absolutely necessary.**

Sensitive personal information is 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, criminal convictions and offenses. BMC will assess whether sensitive personal information is required for the proposed use and whether it is absolutely necessary in the context of its business.

**Rule 7B – BMC will only transfer and use sensitive personal information collected in Europe where the individual's explicit consent has been obtained unless BMC has an alternative legitimate basis for doing so consistent with the applicable law of the European country in which the personal information was collected.**

In principle, individuals must explicitly agree to BMC collecting and using sensitive personal information. This permission to use sensitive personal information by BMC must be genuine and freely given. BMC may also use sensitive personal information if it is required by local law or BMC has another legitimate basis for doing so, consistent with the applicable law of the country in which the personal information was collected.

## SECTION B: PRACTICAL COMMITMENTS

### RULE 8 – COMPLIANCE

**Rule 8 – 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 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 Policy on a day-to-day basis. A summary of the roles and responsibilities of BMC's privacy team is set out in Appendix 2.

### RULE 9 – TRAINING

**Rule 9 – 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 10 – AUDIT

**Rule 10 – BMC will comply with the Controller and Processor Data Protection Binding Corporate Rules Audit Protocol set out in Appendix 4.**

### RULE 11 – COMPLAINT HANDLING

**Rule 11 – BMC will comply with the Controller and Processor Data Protection Binding Corporate Rules Complaint Handling Procedure set out in Appendix 5.**

### RULE 12 – COOPERATION WITH DATA PROTECTION AUTHORITIES

**Rule 12 – BMC will comply with the Controller and Processor Data Protection Binding Corporate Rules Cooperation Procedure set out in Appendix 6.**

### RULE 13 – UPDATE OF THE POLICY

**Rule 13 – BMC will comply with the Controller and Processor Data Protection Binding Corporate Rules Updating Procedure set out in Appendix 7.**

## RULE 14 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

**Rule 14A – BMC will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under Part II of this Policy or such legislation has a substantial effect on its ability to comply with Part II of this 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 outside Europe that has not been recognized by the European Commission as ensuring an adequate level of protection, applicable to the processing of the personal information under Part II of the this Policy, may impinge on the effectiveness of this Policy and thus prevent BMC from fulfilling its obligations under Part II of this Policy or has a substantial effect on the guarantees provided by this Policy.

BMC's assessment will be based on the understanding that any laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with this Policy.

Such assessment will take due account of:

(a) the specific circumstances of the transfer, including the location of the processing, the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal information; the economic sector in which the transfer occurs; the storage location of the information transferred;

(b) the laws and practices of the third country relevant in light of the specific circumstances of the transfer, including those requiring the disclosure of information to public authorities or authorizing access by such authorities, and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards;

(c) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under this Policy, including measures applied during transmission and to the processing of the personal information in the third country. BMC's Group Data Protection Officer shall be informed and involved in the identification of such contractual, technical or organizational safeguards.

BMC will monitor, on an ongoing basis, developments in laws and practices of the third country that could affect the initial assessment and the decisions taken accordingly.

BMC will document the assessment and make it available to the competent Supervisory Authority on request.

For the avoidance of doubt, this section 1 also pertains to onward transfers of personal information to controllers and processors that are not Group Members.

**2. Notification**

If the Group Member acting as the data importer has reasons to believe that it is or has become subject to laws or practices not in line with the requirements under Part II of 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 Part II of this Policy, BMC will promptly inform:

(a) The Group Member in Europe acting as the data exporter; and

(b) BMC's Group Data Protection Officer;

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 the Group Member acting as the data importer, and/or the Group Member acting as the data importer, otherwise have reason to believe that the Group Member acting as the data importer can no longer fulfil its obligations under Part II of this Policy, the Group Member acting as the data exporter and the Group Member acting as the data importer shall promptly identify supplementary measures (such as technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation. BMC's Group Data Protection Officer shall be informed and involved in the identification of such supplementary measures.

The Group Member acting as the data importer and BMC's Group Data Protection Officer will inform all other Group Members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Group Member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

BMC will document the identification of supplementary measures and make it available to the competent Supervisory Authority on request.

**4. Suspension, return and deletion**

If they consider that no appropriate supplementary measures can be ensured or if instructed by the competent Supervisory Authority to do so, the Group Member in Europe acting as the data exporter shall suspend the transfer of personal information. Such suspension shall also apply to all transfers for which the same assessment and reasoning would lead to a similar

result, until compliance is again ensured or the transfer is ended. Unless compliance with the Policy is restored within one month of suspension, personal information that has been transferred prior to the suspension shall at the choice of the Group Member in Europe acting as the data exporter be returned to that Group Member or deleted in its entirety. The same shall apply to any copies of the information. The Group Member acting as the data importer shall certify the deletion of the information to the Group Member in Europe acting as the data exporter. Until the information is deleted or returned, the Group Member acting as the data importer shall continue to ensure compliance with Part II of this Policy. In case of local laws applicable to the Group Member acting as the data importer that prohibit the return or deletion of the transferred personal information, the Group Member acting as the data importer warrants that it will continue to ensure compliance with Part II of this Policy and will only process the information, to the extent and for as long as required under that local law.

**Rule 14B – BMC will take appropriate action if (i) it receives a legally binding request for the disclosure of personal information transferred pursuant to Part II of this Policy from a public authority (e.g. a law enforcement authority or state security body), including judicial authorities under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection ("Request for Disclosure") or (ii) becomes aware of any direct access by public authorities to personal information transferred pursuant to this Policy in accordance with the laws of a third country.**

**1. Notification**

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

(a) The Group Member in Europe acting as the data exporter;

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

(c) where possible, the individuals concerned.

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

BMC will put the Request on hold and inform the lead Supervisory Authority who approved this Policy (i.e., the CNIL), unless prohibited from doing so by a law enforcement authority or agency.

If BMC is prohibited from notifying the Group Member in Europe acting as the data exporter and/or the individuals concerned, and/or prohibited from informing the lead Supervisory Authority, under the laws of the third country not recognized by the European Commission as ensuring an adequate level of protection, 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 upon request of the Group Member acting as the data exporter.

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 Group Member in Europe acting as the data exporter and to the competent Supervisory Authority (e.g. number of Requests, type of data requested, requesting authorities, whether Requests have been challenged and the outcome of such challenges if possible, etc.), to the extent that BMC has been authorized by the requesting authority to disclose such information. If BMC is or becomes partially or completely prohibited from providing Group Member in Europe acting as the data exporter with the aforementioned information, it will, without undue delay, inform the Group Member in Europe acting as the data exporter accordingly.

BMC will preserve the abovementioned information for as long as personal information is subject to the safeguards provided by this Policy and will make it available to the Competent Supervisory Authority upon request.

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

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring BMC to transfer or disclose personal information may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or an EU Member State, without prejudice to other grounds for transfer pursuant to GDPR.

**2. Review of legality and minimization**

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 not recognized by the European Commission as ensuring an adequate level of protection, 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 European Commission as ensuring an adequate level of protection, make the documentation available

to the Group Member established in Europe. BMC shall make the same documentation available to the competent Supervisory Authority on request.

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

## RULE 15 – NON-COMPLIANCE AND TERMINATION

**Rule 15A – BMC will take appropriate action if a Group Member acting as an importer is in breach of this Policy or unable to comply with this Policy.**

BMC will not transfer personal information to a Group Member acting as an importer under this Policy, unless that Group Member is effectively bound by the Policy and can deliver compliance.

The Group Member acting as an importer will promptly inform the Group Member acting as an exporter if it is unable to comply with this Policy, for whatever reason, including the situations further described under Rule 14 above.

In case a Group Member acting as an importer is in breach of the Policy or unable to comply with it, the Group Member acting as an exporter will suspend the transfer of personal information.

The Group Member acting as an importer will, at the choice of the Group Member acting as an exporter, immediately return or delete the personal information that has been transferred under the Policy in its entirety, where:

(i) the Group Member acting as an exporter has suspended the transfer, and compliance with this Policy is not restored within a reasonable time, and in any event within one month of suspension; or

(ii) the Group Member acting as an importer is in substantial or persistent breach of this Policy; or

(iii) the Group Member acting as an importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the Policy.

The same commitments will apply to any copies of the personal information transferred under this Policy. The Group Member acting as an importer will certify the deletion of the personal information to the Group Member acting as an exporter.

Until the personal information is deleted or returned, the Group Member acting as an importer will continue to ensure compliance with this Policy. In case of local laws applicable to the Group Member acting as an importer prohibiting the return or deletion of the transferred personal information, the Group Member acting as an importer will continue to ensure

compliance with the Policy, and will only process the data to the extent and for as long as required under that local law.

**Rule 15B – In case a Group Member acting as an importer ceases to be bound by the Policy, that Group Member will keep, return, or delete personal information it received under Part II of this Policy.**

In case a Group Member acting as an importer ceases to be bound by the Policy, the Group Member acting as an exporter and the Group Member acting as an importer will determine if the personal information transferred under the Policy will be kept, returned or deleted.

If the Group Member acting as an exporter and the Group Member acting as an importer agree that the personal information must be kept by the Group Member acting as an importer, protection must be maintained in accordance with Chapter V GDPR.

## SECTION C: THIRD-PARTY BENEFICIARY RIGHTS

European data protection law states that individuals whose personal information is transferred under this Policy may enforce the following elements of Part II of this Policy as third-party beneficiaries:

- data protection principles, lawfulness of processing, security and personal information breach notifications, restriction on onward transfers (Rules 2B, 2C, 3, 4, 6 and 7 of Part II of this Policy);
- transparency and easy access to the Policy (Section C of Part II of this Policy);
- rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (Rules 2A and 5 of Part II of this Policy);
- obligations in case of local laws and practices affecting compliance with this Policy and in case of government access requests (Rule 14 of Part II of this Policy);
- right to complain through BMC's internal complaint process (Rule 11 of Part II of this Policy);
- cooperation duties with Supervisory Authorities (Rule 12 of Part II of this Policy) relating to compliance obligations covered by this Section;
- duty to inform individuals about any update of the Policy and the list of Group Members (Rule 13 of Part II of this Policy)
- jurisdiction and liability provisions, including the right to judicial remedies, redress and compensation (Section C of Part II of this Policy).

It is agreed that such third-party beneficiary rights shall not be open to 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 individual defined hereabove who benefits from this third-party beneficiary right shall be entitled to seek the following actions:

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

(b) *Complaints to the Supervisory Authority*: Individuals may lodge a complaint to a competent Supervisory Authority in the jurisdiction of the European Member State where the individual has his habitual residence, place of work or in the place of the alleged infringement.

(c) *Jurisdiction:* Individuals may bring proceedings against BMC before the competent court of the European Member States where:

- the Group Member has an establishment;
- the provider of a service, acting as a processor, has an establishment; or alternatively
- the individual has his or her habitual residence.

(d) *Liability:* Individuals may seek appropriate redress from a Group Member including the judicial remedy of any breach of the elements listed above by any provider of a service, acting as a controller or a processor, and, where appropriate receive compensation from a Group Member for any damage suffered as a result of a breach of the elements listed above in accordance with the determination of a court or other competent authority. Individuals may be represented by a not-for-profit body, organization or association under the conditions set out in the GDPR.

It is agreed that, should the Group Member who caused the damage be located outside the European Union, the European Group Member who acted as the exporter 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 damages resulting from a violation of the above listed elements of the Policy by such Group Member located outside the European Union. The European Group Member who acted as the exporter will accept liability as if the violation had been caused by him in the European Member State in which he is based instead of the Group Member established outside the European Union.

(e) Transparency *and Easy Access to the Policy*: Individuals benefiting from third party beneficiary rights shall be provided with an access to this Policy on www.bmc.com and on BMC's employee intranet.

(f) *Burden of Proof:* In the event of a claim being made in which an individual has suffered damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of the Introduction to the Policy or Part II or IV of the Policy, BMC has agreed that the burden of proof to show that the Group Member acting as an importer is not responsible for the breach, or that no such breach took place, will rest with the Group Member acting as an exporter.

# PART III: BMC AS A PROCESSOR

Part III of the Policy applies in all cases where BMC collects, uses and transfers personal information as a processor on behalf of a third party under a contract evidenced in writing, in a situation where the third party will be a controller (referred to as the "**Client**" in Part III of this Policy). Clients are also referred to as "**Controllers**" in Part III of this Policy.

The principal areas in which BMC acts as a processor include the provision of software as a service.

When BMC acts as a processor, the controller retain the responsibility to comply with European data protection law. Certain data protection obligations are passed to BMC in the contracts BMC has with its Clients, in accordance with applicable law. If BMC fails to comply with such data protection obligations, BMC may face a civil claim for breach of contract which may result in the payment of compensation or other judicial remedies, as well as an administrative sanction for a breach of applicable data protection law. If a Client demonstrates that it has suffered damage, and that it is likely that the damage occurred because of a breach of Part III of the Policy (or any of the commitments in the Introduction to the Policy or the appendices in Part IV of the Policy (as applicable)) by a Group Member outside Europe or a third party sub-processor established outside Europe, that Client is entitled to enforce this Policy against BMC. In such cases, the obligation will be on the Group Member accepting liability (namely the Group Member which is a party to a contract with the Client) to show that a Group Member outside Europe (or a third party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place.

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

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

(i) Personal information subject to European Union law; or

(ii) All personal information whatever the origin of the personal information.

Part III of the Policy is divided into three sections:

- **Section A**: addresses the basic principles that BMC must observe when BMC collects and uses personal information as a processor.
- **Section B**: deals with the practical commitments made by BMC to the Supervisory Authorities when BMC collects and uses personal information.
- **Section C:** describes the third-party beneficiary rights that BMC has granted to individuals in its capacity as a processor under Part III of the Policy.

## SECTION A: BASIC PRINCIPLES

### RULE 1 – COMPLIANCE WITH LOCAL LAW AND ACCOUNTABILITY

**Rule 1A – BMC will ensure that compliance with Part III of the Policy will not conflict with applicable data protection laws where they exist.**

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

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

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

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

BMC will maintain a written record of the processing activities carried out on behalf of its Clients, in line with the requirements set out in applicable law and which may be made available to Supervisory Authorities upon their request.

The record shall contain:

- the name and contact details of the Group Member acting as the processor or processors and of each Client on behalf of which the Group Member is acting, and, where applicable, of the Client's representative, and the data protection officer;
- the categories of processing carried out on behalf of each Client;

- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization;

- where possible, a general description of the technical and organizational security measures applicable to processing.

BMC will make available to its Clients all information necessary to demonstrate compliance with its obligations under applicable law, and will allow for and contribute to audits, including inspections conducted by the Client, in accordance with the terms of the contract with such Client.

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

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

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

BMC will assist its Clients in complying with such requirements, within the limits of applicable law and as per the terms of its contracts with its Clients. For example, BMC may be required by applicable law to provide information about any sub-processors appointed by BMC to process Client personal information on its behalf, in which case the terms of such communication shall be detailed in the contract with that particular Client.

**Rule 2B – BMC will only use personal information on behalf of and in accordance with the specific instructions of its Clients ("Purpose limitation").**

BMC will only use personal information in compliance with the terms of a contract it has with its Client, unless otherwise required by European Union or the Member State law applicable to BMC.

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

If, for any reason, BMC is unable to comply with this Rule or its obligations under Part III of the Policy in respect of any contract it may have with a Client, BMC will inform that Client promptly of this fact. BMC's Client may then suspend the transfer of personal information to BMC and/or terminate the contract, depending upon the terms of its contract with BMC.

On the termination of the provision of services to a Client, BMC will, at the choice of the Client, delete or return all, personal information to the Client and delete the copies thereof, as

required in accordance with the terms of its contract with that Client, unless European Union or Member State law requires storage of personal information by BMC. In that case, BMC will maintain the confidentiality of the personal information and will no longer actively process that personal information, i.e., for the purposes for which it was initially collected.

## RULE 3 – DATA QUALITY AND PROPORTIONALITY

**Rule 3 – BMC and its sub-processors will assist its Clients to keep the personal information accurate and up to date.**

BMC will comply with any instructions from a Client, as required by applicable law and under the terms of its contract with that Client, in order to assist them to comply with their obligation to keep personal information accurate and up to date.

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

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

## RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

**Rule 4 – BMC will assist its Clients to comply with the rights of individuals.**

BMC will act in accordance with the instructions of a Client as required under the terms of its contract with that Client and undertake any appropriate technical and organizational measures to enable its Clients to comply with their duty to respect the rights of individuals. In particular, if BMC receives an individual's rights request, it will transfer such request promptly to the relevant Client and not respond to such a request unless authorized to do so or required by law.

## RULE 5 – SECURITY AND CONFIDENTIALITY

**Rule 5A – BMC will put in place appropriate technical and organizational measures to safeguard personal information processed on behalf of its Clients to ensure a level of security appropriate to the risk.**

European law expressly requires that where BMC provides a service to a Client which involves the processing of personal information, the contract between BMC and its Client details the security and organizational measures required to safeguard that information in a manner appropriate with the associated level of risk and consistent with the law of the European country from which the personal information was transferred.

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

BMC will notify a Client of any personal information breach in relation to personal information processed on behalf of that Client without undue delay and as required to do so under the terms of the contract with that Client. Furthermore, any personal information breach shall be documented in accordance with applicable law (including the facts relating to the breach, its consequences and the remedial action taken). Such documentation will be made available to the Supervisory Authority upon request of the Client, and as per the terms of the contract with such Client.

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

BMC will inform its Clients where processing undertaken on their behalf will be conducted by a sub-processor, whether such sub-processor is a Group Member or an external service provider, and will comply with the particular requirements of a Client with regard to the appointment of sub-processors as set out under the terms of its contract with that Client. BMC will ensure that up to date information regarding its appointment of sub-processors is available to those Clients at all times and to obtain their general written consent for such sub-processing. If a Client objects to the appointment of a sub-processor to process personal information on its behalf, that Client will be entitled to require from BMC that the transfer of personal information be suspended and/or to terminate the contract, depending on the terms of its contract with BMC.

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

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

To comply with this Rule, where a sub-processor has access to personal information processed on behalf of BMC, BMC will take steps to ensure that it has in place appropriate technical and organizational security measures to safeguard the personal information in accordance with applicable law and will impose strict contractual obligations in writing on the sub-processor which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in Part III of the Policy (and in particular

Rules 5A and 5B above) and with the terms of the contract BMC has with a Client in respect of the processing in question;

- that the sub-processor will act only on BMC's instructions when using that information including with regard to transfers of personal information to a third country or an organization outside Europe;

- that the sub-processor will cooperate with the Supervisory Authorities and the Client in a similar way as BMC as detailed in part III of the Policy; and

- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by BMC in Part III of the Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of personal information from a Group Member in Europe to a sub-processor established outside Europe.

Contracts with sub-processors will include in particular:

- a requirement to process personal information based solely on Client's instructions;

- the rights and obligations of the Client;

- the scope of processing (duration, nature, purpose and the categories of personal information);

- an obligation for the sub-processor to:

    - implement appropriate technical and organizational measures to protect the personal information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access;

    - provide full cooperation and assistance to Client to allow individuals to exercise their rights under the BCR;

    - provide full cooperation to Client so they can demonstrate its compliance obligations – this includes the right of audit and inspection;

    - make all reasonable efforts to maintain the personal information so that they are accurate and up to date at all times;

    - return or delete the data at the request of a Client, unless required to retain some or part of the data to meet other legal obligations; and

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

## SECTION B: PRACTICAL COMMITMENTS

### RULE 6 – COMPLIANCE

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

BMC has appointed a Group Data Protection Officer who is part of the Core Privacy Team to oversee and ensure compliance with the 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 Policy on a day-to-day basis. A summary of the roles and responsibilities of BMC's privacy team is set out in Appendix 2.

### RULE 7 – TRAINING

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

### RULE 8 – AUDIT

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

### RULE 9 – COMPLAINTS

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

### RULE 10 – COOPERATION WITH DPAs

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

### RULE 11 – UPDATES TO PART III OF THE POLICY

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

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

**Rule 12A – BMC will take appropriate action if it believes that the legislation applicable to it prevents it from fulfilling its obligations under Part III of the Policy or such legislation has a substantial effect on its ability to comply with the 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 outside Europe that has not been recognized by the European Commission 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.

Such assessment will take due account of:

(a) the specific circumstances of the transfer, including the location of the processing; the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal information; the economic sector in which the transfer occurs; the storage location of the information transferred;

(b) the laws and practices of the third country relevant in light of the specific circumstances of the transfer, including those requiring the disclosure of information to public authorities or authorizing access by such authorities, and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards;

(c) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under this Policy, including measures applied during transmission and to the processing of the personal information in the third country. BMC's Group Data Protection Officer shall be informed and involved in the identification of such contractual, technical or organizational safeguards.

BMC will monitor, on an ongoing basis, developments in laws and practices of the third country that could affect the initial assessment and the decisions taken accordingly.

BMC will document the assessment and make it available to the competent Supervisory Authority on request.

For the avoidance of doubt, this section also pertains to onward transfers of personal information to controllers and processors that are not Group Members.

## 2. Notification

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

(a) the Client, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority) and the Group Member acting as the data exporter; and

(b) BMC's Group Data Protection Officer;

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 the Client and/or the Group Member acting as the data exporter otherwise have reason to believe that the Group Member acting as the data importer can no longer fulfil its obligations under Part III this Policy, the Client, the Group Member acting as the data exporter and the Group Member acting as the data importer shall promptly identify supplemental measures (such as technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation.

BMC's Group Data Protection Officer shall be informed and involved in the identification of such supplementary measures.

BMC will document the identification of supplementary measures and make it available to the competent Supervisory Authority on request.

## 4. Suspension, return and deletion

If the Client or the Group Member acting as the data exporter consider that no appropriate supplementary measures can be ensured or if instructed by the competent Supervisory Authority to do so, or if the Group Member acting as an exporter is unable to comply with this Policy, for whatever reason, the Client or the Group Member acting as the data exporter shall suspend the transfer of personal information. Such suspension shall also apply to all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended. Unless compliance with the Policy is restored within one month of suspension, personal information that has been transferred prior to the suspension shall at the choice of the Client immediately be returned to that Client or deleted in its entirety. The same shall apply to any copies of the information. The Group Member acting as the data importer shall certify the deletion of the information to the Client. Until the information is deleted or returned, the Group Member acting as the data importer shall continue to ensure compliance with Part III of this Policy. In case of local laws applicable to

the Group Member acting as the data importer that prohibit the return or deletion of the transferred personal information, the Group Member acting as the data importer warrants that it will continue to ensure compliance with Part III of this Policy and will only process the information, to the extent and for as long as required under that local law.

**Rule 12B – BMC will take appropriate action if (i) it receives a legally binding request for the disclosure of personal information transferred pursuant to Part III of this Policy from a public authority (e.g. a law enforcement authority or state security body), including judicial authorities under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection ("Request for Disclosure") or (ii) becomes aware of any direct access by public authorities to personal information transferred pursuant to Part III this Policy in accordance with the laws of a third country**

**1. Notification**

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

(a) the Client, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority) and the Group Member acting as an exporter;

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

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

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

BMC will put the Request on hold and inform the lead Supervisory Authority who approved this Policy (i.e., the CNIL) and the appropriate Supervisory Authority competent for the Client, unless prohibited from doing so by a law enforcement authority or agency

If BMC is prohibited from notifying the Client and/or the individuals concerned, and/or prohibited from informing the competent Supervisory Authorities, under the laws of the third country not recognized by the European Commission as ensuring an adequate level of protection, BMC will use its best efforts to obtain a waiver of the prohibition. BMC will document its best efforts in order to be able to demonstrate them on request of the Client or of the Group Member acting as the data exporter.

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 Client and to the competent Supervisory Authorities (e.g. number of Requests, type of data requested, requesting authorities, whether Requests have been challenged and the outcome

of such challenges if possible, etc.), to the extent that BMC has been authorized by the requesting authority to disclose such information. If BMC is or becomes partially or completely prohibited from providing the Client or the Group Member in Europe acting as the data exporter with the aforementioned information, it will, without undue delay, inform the Client and the Group Member in Europe acting as the data exporter accordingly.

BMC will preserve the information pursuant to this section 1 for the duration of the service agreement with the Client and make it available to the competent Supervisory Authority on request.

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

**2. Review of legality and minimization**

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 not recognized by the European Commission as ensuring an adequate level of protection, 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 European Commission as ensuring an adequate level of protection, make the documentation available to the Client. BMC shall make the same documentation available to the competent Supervisory Authority on request.

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

European data protection law states that individuals located in the European Union must be given rights to enforce Part III of this Policy as third-party beneficiaries.

It is agreed that such third-party beneficiary rights shall not be open to individuals which personal information is not handled by BMC acting as a processor.

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

- duty to respect the instructions from the controller regarding the personal information processing including for data transfers to third party (Rule 2B Part III of this Policy);
- duty to implement appropriate technical and organizational security measures and to notify any personal information breach to the controller (Rules 5A and 5B Part III of this Policy);
- duty to respect conditions when engaging a sub-processor either within or outside the Group Members (Rules 5C and 5D Part III of this Policy);
- duty to cooperate with and assist the controller in complying and demonstrating compliance with applicable law (Rules 1B and 4 Part III of this Policy);
- easy access to this Policy (Section C Part III of this Policy);
- right to complain through internal complaint mechanisms (Rule 9 Part III of this Policy);
- duty to cooperate with the Supervisory Authority (Rule 10 Part III of this Policy);
- liability, compensation and jurisdiction provisions (Section C Part III of this Policy); and
- national legislation preventing respect of this Policy (Rule 12 Part III of this Policy).

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

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

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

(b) *Complaints to the Supervisory Authority*: individuals may make a complaint to the Supervisory Authority in the jurisdiction of the individual's habitual residence, place of work or place of alleged infringement.

(c) *Jurisdiction*: Individuals may bring proceedings against BMC before the competent court of the European Member States where:

(i) the controller has an establishment;

(ii) BMC acting as a processor has an establishment; or

(iii) the individual has his or her habitual residence.

(d) *Liability*: It is agreed that, should a BMC Group Member acting as a processor, or a sub-processor, be located outside the European Union, the Group Member acting as an exporter shall accept responsibility for and agree to take the necessary action to remedy the acts of the processor, the sub-processor and/or the controller in the limited cases mentioned above, and to pay compensation for any damages resulting from a violation of the above elements of the Policy. The European Group Member will accept liability as if the violation had taken place by him in the European Member State in which the is based instead of the processor or the sub-processor established outside the European Union, and/or the controller.

Where the individual has engaged a proceeding against the processor instead of the controller, the concerned individual shall be entitled to receive compensation for the entire damage directly from the processor, even though the processor may not be responsible for any of the damage caused.

Where the processor and the controller involved in the same proceeding are found liable for damages, the concerned individual shall be entitled to receive compensation for the entire damage directly from the processor.

The processor or sub-processor may not rely on a breach by the controller or a subsequent sub-processor (internal or external of the group) of its obligations to avoid its own liability.

(e) *Transparency and Easy access to Policy:* All concerned individuals benefiting from third-party beneficiary rights shall be provided with the information on such third-party beneficiary rights with regard to the processing of their personal information and on the means to exercise those rights via a publication of the Policy on www.bmc.com.

(f) *Burden of proof:* Where a Group Member outside Europe is acting as a processor on behalf of a third party controller or should an external sub-processor be used, in the event that an individual suffers damage where that individual or controller can demonstrate that it is likely that the damage has occurred because of a breach of the rights detailed hereabove, the burden of proof to show that such Group member acting as a sub-processor or any third party sub-processor which is

established outside Europe and which is acting on behalf of a Group Member is not responsible for the breach, or that no such breach took place, will rest with a European Group Member. If the European Group Member can prove that the Group Member acting as sub-processor or any third party sub-processor which is established outside the European union is not responsible for the act, it may discharge itself from any responsibility.

# PART IV: APPENDICES

## APPENDIX 1 - INDIVIDUALS' RIGHTS REQUESTS PROCEDURE

### 1. Introduction

1.1 When BMC collects, uses 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 located in Europe[3] 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 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.

1.4 Where a Request is subject to European data protection law because it is made with respect to individuals located in Europe, such Request will be dealt with by BMC in accordance with this Procedure, but where the applicable data protection law differs from this Procedure, the local data protection law will prevail.

1.5 When BMC processes information on behalf of a controller (for example, to provide a service), BMC is deemed to be a processor of the information and the controller will be primarily responsible for meeting the legal requirements of a controller. This means that when BMC acts as a processor, the controller retains the responsibility to comply with applicable data protection law.

[3] In this Procedure, Europe means the EEA.

1.6 Certain data protection obligations are passed to BMC in the contracts BMC has with its Clients, and in that case, BMC must act in accordance with the instructions of its Client and undertake any reasonably necessary measures to enable the Client to comply with its duty to respect the rights of individuals. This means that if BMC receives an individual right request in its capacity as a processor for a Client, BMC must transfer such request promptly to the relevant Client and not respond to the request unless authorized by such Client to do so.

1.7 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. BMC shall inform the individual about such rectification, erasure or restriction, and shall inform the individual about such recipients upon request.

## 2. General Process

2.1 Requests must be made in writing (where required), which can include email[4]. 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.

[4] Unless the local data protection law provides that an oral request may be made, in which case BMC will document the request and provide a copy to the individual making the request before dealing with it.

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

(a) Where the Request was made to a European Group Member and relates to personal information held by that Group Member, and:

- The Request is manifestly unfounded or excessive; or
- The execution of the Request would adversely affect the rights and freedoms of others;

(b) Where the Request was made to a non-European Group Member and relates to personal information held by that Group Member, and:

- 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 does not originate from Europe 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 or by mail to: BMC Software, Group Data Protection Officer, Cœur Défense - Tour A, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, France.

**3. Right of Access**

3.1 Individuals are entitled to obtain:

(a) confirmation as to whether or not personal information relating to them are being processed and, where that is the case;

(b) 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 the European Commission 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 a Supervisory Authority;

- any available information as to the source of personal information which had not been collected from the individual;

- 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:

(a) personal information is no longer necessary in relation to the purposes for which it was collected or otherwise processed; or

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

(c) 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; or

(d) personal information has been unlawfully processed; or

(e) personal information must be erased for compliance with a legal obligation in European or Member State law to which BMC is subject;

(f) personal information has been collected in relation to the offer of information society services to children.

**6. Right to Restrict Processing**

6.1 Individuals are entitled to obtain restriction of processing, where:

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

(b) the processing is unlawful and the individual opposes the erasure of the personal information and requests the restriction of their use instead;

(c) 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 defense of legal claims; or

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

**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:

(a) personal information is processed based on consent or on a contract with the individual; and

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

**8. Right to Object**

8.1 Individuals are entitled to object, on particular grounds, to processing of their personal information, where personal information:

(a) 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 defense of legal claims;

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

## 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:

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

(b) is authorized by applicable European law; or

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

## 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 and Processor Data Protection Binding Corporate Rules of BMC Software (the "**Policy**") and other privacy related policies, objectives and standards within BMC.

### 1. Executive Steering Committee

This committee consists of 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 Policy, including:

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

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

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

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

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

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

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

### 2. Business Units Representatives

BMC has established a network of Business Units Representatives which consists of mid-level executives and managers from all 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.

Business Units Representatives are responsible for:

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

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

(iii) Ensuring that BMC's business objectives align with the 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**

The Core Privacy Team has primary responsibility for ensuring that BMC complies with the Policy and with global privacy regulations on a day-to-day basis. The group consists of senior BMC employees in the following functional areas: Privacy, EMEA Legal and IT Security.

The Core Privacy Team includes BMC's Group Data Protection Officer. BMC's Group Data Protection Officer will not have any tasks that could result in a conflict of interests and will inform Group Members' highest management level if any questions or problems arising during the performance of his duties.

BMC's Group Data Protection Officer is responsible for monitoring compliance with the Policy and will enjoy the highest management support for the fulfilling of this task. In particular, BMC's Group Data Protection Officer is responsible for:

(i) Informing and advising Group Members on their obligations;

(ii) Monitoring compliance by Group Members;

(iii) Providing advice to Group Members as regards data protection impact assessments;

(iv) Cooperating with Supervisory Authorities; and

(v) Acting as a contact point for Supervisory Authorities.

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

(i) Responding to inquiries and complaints relating to the Policy from individuals assessing the collection and use 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 privacy champions in driving the 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 Policy, coordinating responses to audit findings and responding to inquiries of the Supervisory Authorities.

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

(v) Promoting the 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) Reporting periodically on the status of the Policy to the Executive Steering Committee.

(viii) Hosting and coordinating meetings as necessary.

(ix) Overseeing training for employees on the Policy and on data protection legal requirements in accordance with the requirements of The Controller and Processor Data Protection Binding Corporate Rules of BMC Software Privacy Training Requirements.

(x) Escalating issues relating to the Policy to the Executive Steering Group where required.

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

## 4. Local privacy champions network

BMC has established a network of local privacy champions to assist with the operation of the 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 Policy in their jurisdiction.

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

## APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS

### 1. Background

1.1 The Controller and Processor Data Protection Binding Corporate Rules of BMC Software (the "**Policy**") provide a framework for the transfer of personal information between BMC group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how BMC trains such individuals on the requirements of the Policy.

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

1.3 Employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information receive additional, tailored training on the 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 Policy, such as responding to individuals' rights requests or handling complaints, receive specific training in these areas.

### 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 Policy as described in section 4 below.

### 3. Aims of data protection and privacy training at BMC

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

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

3.1.2 employees understand the Code; and

3.1.3 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 Policy.

3.2 General data protection and privacy training for new joining employees

3.2.1 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.

3.3 General data protection and privacy training for all employees

3.3.1 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 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.

3.3.2 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 Policy

4.1 Employees receive training on the Policy appropriate to their roles and responsibilities within BMC.

4.2 New employees are trained on the Policy as part of their onboarding. Training is regularly delivered to current employees, on a biennial basis or more frequently if necessary.

4.3 BMC's training on the Policy is kept up to date and covers the following main areas:

4.3.1 Background and rationale:

(a) What is data protection law?

(b) How data protection law will affect BMC internationally, including procedures for managing requests for access to personal information by public authorities

(c) The scope of the Policy

(d) Terminology and concepts

4.3.2 The Policy:

(a) An explanation of the Policy

(b) Practical examples

(c) The rights that the Policy gives to individuals

(d) The data protection and privacy implications arising from the processing of personal information on behalf of clients

4.3.3 Where relevant to an employee's role, training will cover the following procedures under the 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

Any queries about training under the 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 and Processor Data Protection Binding Corporate Rules of BMC Software (the "**Policy**") is to safeguard personal information transferred between the BMC group members ("**Group Members**").

1.2 The Policy requires approval from a Supervisory Authority in the European Member States from which the personal information is transferred. One of the requirements of the lead Supervisory Authority who approved this Policy (i.e., the CNIL) is that BMC audits compliance with the 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 use of personal information subject to the Policy and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use 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 Policy as required by the Supervisory Authority, this is only one way in which BMC ensures that the provisions of the Policy are observed and corrective actions taken as required.

### 2. Approach

2.1 Overview of audit

2.1.1 Compliance with the 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 Policy and will ensure that such audits address all aspects of the Policy in accordance with the BMC audit program. 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 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 Policy will take place:

(a) **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 To the extent that a Group Member processes personal information on behalf of a third-party controller, audit of the Policy will take place as required under the contract in place between that Group Member and that third-party controller.

2.2.3 The scope of the audit performed will be determined independently by BMC's **Assurance Department** with consideration given to input received from the **Core Privacy Team** and **Executive Steering Committee** based on the use of a risk-based analysis which will consider relevant criteria, for example: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of the personal information processed.

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

2.3 Auditors

2.3.1 Audit of the Policy will be undertaken by BMC's **Assurance Department.** BMC may utilize other accredited internal or external auditors as determined by BMC. Auditors will be guaranteed independence as to the performance of their duties related to their audit mission. Auditors cannot be used if their designation may result in a conflict of interests.

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

2.3.3 BMC's **Audit Committee** consisting of members of the Board of Directors of BMC Software, Inc. (the "**Board**") is appointed by the Board to assist it in fulfilling its

oversight responsibilities with respect to matters including BMC's legal and regulatory compliance and the performance of internal audit functions and external auditors.

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

2.4 Report

2.4.1 BMC's **Assurance Department** will provide the results of any audit of the Policy to BMC's **Core Privacy Team**, including BMC's Group Data Protection Officer, to the **Executive Steering Committee** and to 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.

2.4.2 BMC has agreed to:

(a) provide copies of the results of any audit of the Policy to a Supervisory Authority of competent jurisdiction upon that Authority's request; and

(b) to the extent that an audit relates to personal information processed by BMC on behalf of a third-party controller, to make the results of any audit of compliance with Part III of the Policy available to that controller.

## APPENDIX 5 - COMPLAINT HANDLING PROCEDURE

### 1. Introduction

1.1 The Controller and Processor Data Protection Binding Corporate Rules of BMC Software (the "Policy") safeguard personal information processed or transferred between the BMC group members ("Group Members"). The content of the Policy is determined by the Supervisory Authorities in the European Member States from which the personal information is transferred and one of their requirements is that BMC must have a complaint handling procedure in place. The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by BMC under the Policy are dealt with.

### 2. How individuals can bring complaints

2.1 Individuals can bring complaints in writing by contacting BMC's Group Data Protection Officer via email to privacy@bmc.com or by mail to: BMC Software, Group Data Protection Officer, Cœur Défense - Tour A, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex, France. These are the contact details for all complaints made under the Policy and whether BMC is collecting and/or using personal information on its own behalf or on behalf of a client.

### 3. Who handles complaints?

3.1 Complaints where BMC is a controller

3.1.1 BMC's Group Data Protection Officer will handle all complaints arising under the Policy where a complaint is brought in respect of the collection and use 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.

3.1.2 What is the response time?

Unless exceptional circumstances apply, BMC's Group Data Protection Officer will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. Such response will include information on actions taken by BMC.

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 reasonable estimate (not exceeding two additional months) for the timescale within which a response will be provided.

3.1.3 When a complainant disputes a finding

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.

3.1.4 Individuals whose personal information is transferred under this Policy also have the right to lodge a complaint to the competent Supervisory Authority located in the Member State of the individual's habitual residence, place of work or place of the alleged infringement; and/or to lodge a claim with a court of competent jurisdiction where BMC has an establishment, or where the individuals have their habitual residence. Individuals may lodge such a claim or complaint whether or not they have first made a complaint to BMC and without having exhausted this Complaint Handling Procedure beforehand.

3.1.5 If the matter relates to personal information which has been exported to a Group Member outside Europe and an individual wants to make a claim against BMC, the claim may be made against the Group Member acting as the data exporter.

3.2 Complaints where BMC is a processor

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

3.2.2 By derogation to the aforementioned, when a client ceases to exist

In circumstances where a client has disappeared factually, no longer exists in law or has become insolvent, BMC will handle such complaints in accordance with section 3.1. of this Complaint Handling Procedure. In such cases, individuals also have the right to complain to the competent Supervisory Authority and/or to lodge a claim with a court of competent jurisdiction and this includes where they are not satisfied with the way in which their complaint has been resolved by BMC. Individuals entitled to such rights will be notified accordingly as part of the Complaint Handling Procedure.

## APPENDIX 6 - COOPERATION PROCEDURE

### 1. Introduction

1.1 This Cooperation Procedure sets out the way in which BMC will cooperate with the European[5] Supervisory Authorities in relation to The Controller and Processor Data Protection Binding Corporate Rules of BMC Software (the “Policy").

### 2. Cooperation Procedure

2.1 Where required, BMC will make the necessary personnel available for dialogue with a Supervisory Authority in relation to the Policy.

2.2 On any issue related to this Policy, Group Members will:

2.2.1 cooperate with, accept to be audited and to be inspected, including where necessary, on-site, by the competent Supervisory Authorities,

2.2.2 take into account their advice, and

2.2.3 abide by decisions of these Supervisory Authorities

2.3 BMC will provide upon request copies of the results of any audit of the Policy and data protection impact assessment to a relevant Supervisory Authority.

2.4 BMC agrees that:

2.4.1 where any BMC group member ("**Group Member**") is located within the jurisdiction of a Supervisory Authority based in Europe, BMC agrees that this Supervisory Authority may audit that Group Member for the purpose of reviewing compliance with the Policy, in accordance with the applicable law of the country in which the Group Member is located; and

2.4.2 in case of a Group Member located outside Europe, BMC agrees that a Supervisory Authority based in Europe may audit that Group Member for the purpose of reviewing compliance with the Policy in accordance with the applicable law of the European country from which the personal information is transferred under the Policy (which, when BMC acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller).

2.4.3 Any dispute related to a Competent Supervisory Authority’s exercise of supervision of compliance with this Policy will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State’s procedural law. Group Members agree to submit themselves to the jurisdiction of these courts.

[5] For the purpose of this Policy, reference to Europe means the EEA (namely the EU Member States plus Norway Iceland and Liechtenstein).

## APPENDIX 7 - UPDATING PROCEDURE

### 1. Introduction

1.1 This Updating Procedure sets out the way in which BMC will communicate changes to The Controller and Processor Data Protection Binding Corporate Rules of BMC Software (the "**Policy**") to the European[6] Supervisory Authorities, data subjects, its clients and to the BMC group members ("**Group Members**") bound by the Policy.

### 2. Material changes to the Policy

2.1 BMC will communicate any material changes to the Policy to relevant Supervisory Authorities via the *Commission nationale de l'informatique et des libertés* ("**CNIL**"), as soon as is reasonably practical. Where a modification would affect the level of the protection offered by the Policy or significantly affect the Policy (i.e., changes in the binding nature of the Policy), it must be communicated in advance.

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

2.3 Updates to the Policy or to the list of the Group Member are possible without having to re-apply for an authorization providing that:

(i) An identified person keeps a fully updated list of the Group Member and of the sub-processors involved in the data processing activities for the controller which shall be made accessible to the data controller, individuals and Supervisory Authorities.

(ii) This person will keep track of and record any updates to the rules and provide the necessary information systematically to the data controller and upon request to Supervisory Authorities upon request.

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

(iv) Any changes to the BCRs or to the list of BCR members shall be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update. Where a modification would affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e., changes in the bindingness), it must be promptly communicated to the competent Supervisory Authority.

[6] References to Europe for the purposes of this document include the EEA.

## 3. Administrative changes to the Policy

3.1 BMC will communicate changes to the Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or Supervisory Authority measure to the CNIL and to any other relevant Supervisory Authorities at least once a year. BMC will also provide a brief explanation to the CNIL and to any other relevant Supervisory Authorities of the reasons for any notified changes to the Policy. In instances where no changes have been made, BMC will notify the CNIL once a year accordingly. In any case, the annual notification will confirm that Group Members have sufficient assets, or have made appropriate arrangements to enable themselves to pay compensation for damages resulting from a breach of this Policy.

3.2 BMC will make available changes to Part III of the Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or Supervisory Authority measure to any client on whose behalf BMC processes personal information.

## 4. Communicating and logging changes to the Policy

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

4.2 BMC will communicate all changes to the Policy, whether administrative or material in nature, without undue delay:

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

4.2.2 systematically to clients on whose behalf BMC processes personal information; and

4.2.3 to data subjects who benefit from the Policy, by publishing the new version on www.bmc.com .

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 Policy and a list of the sub-processors appointed by BMC to process personal information on behalf of its clients. This information will be available on request from BMC.

## 5. New Group Members

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

## APPENDIX 8 – MATERIAL SCOPE

### 1. Introduction

1.1 This Appendix sets out the material scope of the Controller and Processor Data Protection Binding Corporate Rules of BMC Software. 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.

### 2. Material scope as a Controller

2.1 This section sets out the material scope of Part II of the Controller and Processor Data Protection Binding Corporate Rules of BMC Software.

#### 2.1.1 Customer relationship data (Sales & Marketing)

| | |
|---|---|
| Who transfers the personal information described in this section? | Group Members may transfer the personal information that they control described in this section to every other Group Members. |
| Who receives this personal information? | Every BMC Group Member may receive the personal information described in this section which is sent to them by another 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;<br>- Employment information, such as job title, roles and company. |
| What special categories of personal information (if any) are transferred? | BMC does not collect or otherwise process special categories of personal information, as defined by Article 6, 9 and 10 of GDPR. |
| Who are the types of individuals whose personal information are 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);<br><br>Use BMC customers relationship management systems (Lawful basis: BMC's legitimate interest);<br><br>Manage customers clickwrap acceptance of BMC's license agreements (Lawful basis: BMC's legitimate interest);<br><br>Review bid processes (Lawful basis: BMC's legitimate interest);<br><br>Respond to inquiries and requests (Lawful basis: BMC's legitimate interest);<br><br>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);<br><br>Manage export compliance (Lawful basis: BMC's legitimate interest);<br><br>Send satisfaction survey (Lawful basis: BMC's legitimate interest); or<br><br>Process orders for billing, booking, accounting and invoicing purposes (Lawful basis: BMC's legitimate interest). |
| Where is this personal information processed? | The personal information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9. |

### 2.1.2 Human Resources data

| | |
|---|---|
| Who transfers the personal information described in this section? | Group Members may transfer the personal information that they control described in this section to every other Group Member. |
| Who receives this personal information? | Every Group Member may receive the personal information described in this section which is sent to them by another Group Member. |
| What categories of personal information are transferred? | - Personal Identification, such as first name, second name and date of birth;<br>- Contact Information, such as home address, contact telephone numbers (landline and mobile) and personal email address;<br>- Education & Skills, such as employment and education history including qualifications, job application, employment references;<br>- Family Information, such as emergency contacts and contact information;<br>- 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;<br>- User Account Information, such as employee ID and credentials,<br>- Geographical Information, such as location of employment;<br>- Financial Information, including compensation, payroll, benefits, expenses or other payments claimed and bank account details;<br>- Government Identifiers, such as passport and national ID;<br>- Citizenship or Immigration Status;<br>- IT systems monitoring, such as logs; and<br>- Photos and CCTV images. |
| What special categories of personal information (if any) are transferred? | - Health information, such as accident records and health management questionnaires, to the extent authorized by applicable Member State law. Processing of health information is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of |

| | |
|---|---|
| | employment and social security and social protection 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 on the basis of applicable Member State law. Such Personal Information is collected and otherwise processed in accordance with Article 6 and 9 of GDPR. Health information is subject to an obligation of secrecy under applicable Member State law.<br><br>- Criminal offence information, to the extent authorized by applicable Member State law providing for appropriate safeguards for the rights and freedom of individuals. 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 GDPR. |
| Who are the types of individuals whose personal information are transferred? | Applicants and employees (both current and former). |
| Why is this personal information transferred and how will it be processed? | BMC has approximately 1000 employees in Europe. HR activities are managed both at local, regional and global levels, for the purposes and in accordance with the lawful basis described below:<br><br>- 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);<br><br>- 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);<br><br>- 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);<br><br>- Administer corporate credit card program and reimburse business expenses (Lawful basis: BMC's legitimate interest);<br><br>- 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);<br><br>- Assign desks, drawers and corporate devices such as mobiles and laptops (Lawful basis: BMC's legitimate interest);<br><br>- Provide IT tools and services to employees, including email and other collaboration tools (Lawful basis: BMC's legitimate interest);<br><br>- 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);<br><br>- Monitor business mobile costs (Lawful basis: BMC's legitimate interest);<br><br>- Provide company lease cars and fuel cards (Lawful basis: BMC's legitimate interest);<br><br>- 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);<br><br>- Maintain BMC organizational charts (Lawful basis: BMC's legitimate interest);<br><br>- Issue emergency communications and maintain business continuity in case of an emergency situation, including relocation to recovery site (Lawful basis: BMC's legitimate interest);<br><br>- Perform financial planning, accounting and tax management (Lawful basis: BMC's legitimate interest);<br><br>- 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);<br><br>- 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);<br><br>- Interact with local works councils (Lawful basis: Compliance with a legal obligation);<br><br>- Monitor compliance with company policies and procedures, including training, internal controls, assessments, questionnaires, testing and BMC Ethics Helpline (Lawful basis: BMC's legitimate interest);<br><br>- 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 1000 employees in Europe. HR activities are managed both at local, regional and global levels.<br><br>The personal information described in this section may be processed in every territory where BMC Group Members or their processors are located. A list of BMC Group Member locations is available at Appendix 9. |

### 2.1.3 Supplier / Vendor data

| | |
|---|---|
| Who transfers the personal information described in this section? | Group Members may transfer the personal information that they control described in this section to every other 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 another Group Member. |
| What categories of personal information are transferred? | Personal details;<br><br>Contact details;<br><br>Goods and services provided;<br><br>Financial details;<br><br>Employment information;<br><br>Education and training details. |
| What special categories of personal information (if any) are transferred? | BMC does not collect or otherwise process special categories of personal information, as defined by Articles 6, 9 and 10 of GDPR. |
| Who are the types of individuals whose personal information are 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:<br>- Procurement management, including supplier selection and due diligence activities (Lawful basis: BMC's legitimate interest);<br>- Engage in and process transactions (Lawful basis: BMC's legitimate interest);<br>- Use BMC supplier management systems (Lawful basis: BMC's legitimate interest);<br>- Manage supplier acceptance of BMC's agreements (Lawful basis: BMC's legitimate interest);<br>- Respond to inquiries and requests (Lawful basis: BMC's legitimate interest);<br>- Manage export compliance (Lawful basis: Compliance with a legal obligation);<br>- 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. |

### 2.1.4 Business Partners / Resellers data

| | |
|---|---|
| Who transfers the personal information described in this section? | Group Members may transfer the personal information that they control described in this section to every other 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 another Group Member. |
| What categories of personal information are transferred? | Personal details, Contact details. |

| | |
|---|---|
| What special categories of personal information (if any) are transferred? | BMC does not collect or otherwise process special categories of personal information, as defined by Articles 6, 9 and 10 of GDPR. |
| Who are the types of individuals whose personal information are 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:<br>- 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. |

## 3. Material scope as a Processor

3.1 This section sets out the material scope of Part III of the Controller and Processor Data Protection Binding Corporate Rules of BMC Software.

### 3.1.1 Customer data

| | |
|---|---|
| Who transfers the personal information described in this section? | Group Members may transfer the personal information that they process described in this section to every other Group Member, subject to Controller's instructions. |
| Who receives this personal information? | Every Group Member may receive the personal information described in this section, which is sent to them by another Group Member, subject to Controller's instructions. |
| What categories of personal information are transferred? | The extent of Customer data processed and transferred by BMC is determined and controlled by Customer in its sole discretion. It will include Personal Information relating to the following categories of Personal Information:<br>• Contact details, such as name, professional phone number, professional email address, professional office address, title, degree, date of birth.<br>• Product usage data, such as media used, file type used, file size, usage and status and information related to BMC Products such as location, language, software version, data sharing choices and update details.<br>• Connection data, such as number of times customer contact has engaged BMC Support centers, duration of the engagement, means by which customer contacted BMC (by email, videoconference, Support centers, etc.), region, language, time zone, localization.<br>• Device data, such as information about Computers, and/or devices such as operating system, amount of memory, region, language, time zone, model number, first start date, age of Computer and/or device, device manufacture date, browser version, computer manufacturer, connection port, device identifiers and additional technical information that varies by Product. |

| | |
|---|---|
| | • Other Personal Information provided by an individual when she/he interacts, online or by phone, or mail with the Support centers, help desks and other customer support channels to facilitate delivery of BMC Services and to respond to Customer or individual inquiries.<br>• Any other Personal Information Customer or Customer's Users submit, send or store via BMC Subscription Services. |
| What categories of sensitive personal information (if any) are transferred? | No sensitive personal information is knowingly processed by BMC. |
| Who are the types of individuals whose personal information are transferred? | - Prospects, customers, business partners and vendors of customer;<br>- Customer’s personnel, including employees, agents and contractors;<br>- Customer’s users authorized by customer to use BMC Services.<br><br>No children’s personal information is knowingly processed by BMC. |
| What categories of sensitive personal information (if any) are transferred? | No sensitive personal information is knowingly processed by BMC. |
| Who are the types of individuals whose personal information are transferred? | - Prospects, customers, business partners and vendors of customer;<br>- Customer’s personnel, including employees, agents and contractors;<br>- Customer’s users authorized by customer to use BMC Services.<br>No children’s personal information is knowingly processed by BMC. |

| | |
|---|---|
| Why is this personal information transferred and how will it be processed? | BMC Products and Services are delivered at local, regional and global levels, and include the provision of:<br>- Software as a Service and cloud computing products;<br>- outsourced helpdesk services;<br>- customer support activity;<br>- educational services;<br>- analytics products; and<br>- services to members of the BMC group of companies.<br><br>BMC uses a tiered support structure to ensure Customers get the best responses to their support requests as quickly as possible. BMC support is always available 24x7x365. BMC use a Follow the Sun approach to ensure Customers have access to Customer Support 24 hours a day through Regional Support Centers strategically placed in Asia-Pacific, Australia, Europe, Latin America, and the United States. After regular business hours of a given support location, severity one tickets are transferred to another support center located in a different time zone.<br><br>Customer support activities include:<br><br>- Performing detailed case analysis;<br><br>- Reproducing customer problems;<br><br>- Developing and providing workarounds and resolutions to customers;<br><br>- Escalating issues to Level 3 support or development;<br><br>- Maintaining ftp and web site content - product patches/fixes and information distribution sites;<br>- Creating failures and requests associated with Customer cases and providing status information to the affected customers. |
| 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. |

## 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) |
|---|---|---|---|---|---|
| Austria | BMC Software GmbH | FN 12295 k | Teinfaltstraße 8, 4th floor, 1010 Vienna, Austria | Privacy@bmc.com | Categories listed in Appendix 8 |
| Belgium | BMC Software Belgium N.V. | BE 424902956 | Botanic Tower - 6th floor, Boulevard Saint-Lazare, 4-10, 1210 Brussels, 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<br>00560, Helsinki, Finland | | |
| France | BMC Software France SAS | 313400681 | Coeur Defense, 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 | | |
| Greece | BMC Software Hellas MEPE | 9300937852 | 1 Alamanas & Delfon, 15125 Marousi, Greece | | |
| Ireland | BMC Software Ireland Unlimited | 481578 | 3 The Campus, Cherrywood,<br>Dublin, Ireland | | |
| Italy | BMC Software S.r.l | 1222185 | Corso Vercelli 40, Milan,<br>20145, Italy | | |

| Country | Group Member name | Registration number | Registered Office address | Contact email (common) | Expected categories of data transferred (common) |
|---|---|---|---|---|---|
| Norway | BMC Software AS | AS-979803125 | Hagaløkkveien 26, 1383 Asker, Norway | Privacy@bmc.com | Categories listed in Appendix 8 |
| Poland | BMC Software Sales (Poland) Sp.z.o.o. | 18835 | Zlota 59, Office #602, Warszaw 00-120, Poland | | |
| 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 | | |
| Sweden | BMC Software AB | 556207-5795 | Vasagatan 38 (3rd floor), 111 20, Stockholm Sweden | | |
| 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 | | |
| The United Kingdom | BMC Software Limited | 01927903 | 13th floor, 1 Angel Court, EC2R 7HJ London, United Kingdom | | |
| Argentina | BMC Software de Argentina S.A. | 1694851 | Ing. Butty 220 - Piso 18, Capital Federal, Buenos Aires, C1001AFB, Argentina | | |

| Country | Group Member name | Registration number | Registered Office address | Contact email (common) | Expected categories of data transferred (common) |
|---|---|---|---|---|---|
| Australia | BMC Software (Australia) Pty. Ltd. | ABN12 007 280 088 | Level 13/383, Kent Street, Sydney, NSW 2000, Australia | Privacy@bmc.com | Categories listed in Appendix 8 |
| Brazil | BMC Software do Brasil Ltda. | 00.723.020/0001-90 | Av. Rebouças 3.970 e Av. Dra Ruth Cardoso, 8.501, 22º Andar, Pinheiros, São Paulo, SP 05425-070, Brazil | | |
| Canada | BMC Software Canada Inc. | 1654693 | 150 King Street West, Suite 306-02, Toronto, Ontario, Canada | | |
| China | BMC Software (China) Limited | 91110101600086987G | Level 38, China World Tower B, No.1, Jianguomenwai Avenue, Chaoyang District, Beijing, 100004 | | |
| | 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 | | |
| Hong Kong | BMC Software (Hong Kong) Limited | 543682 | Level 23, One Island East, No.18 Westlands Road, Taikoo Place, Quarry Bay, Hong Kong | | |

| Country | Group Member name | Registration number | Registered Office address | Contact email (common) | Expected categories of data transferred (common) |
|---|---|---|---|---|---|
| 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 | Privacy@bmc.com | Categories listed in Appendix 8 |
| Israel | BMC Software Israel LTD | 52-003784-7 | 10 Habarzel Street, P. O. Box 58168, 6158101, Tel Aviv, Israel | | |
| Japan | BMC Software K.K. (Japan) | 3011201009842 | Harmony Tower 24F, 1-32-2 Honcho, Nakano-ku, Tokyo, 164-872, Japan | | |
| 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 | | |
| Mexico | BMC Software de Mexico, S.A. de C.V. | Mercantile Folio 248373 | Volcán 150, Piso 2, Oficina 202, Colonia Lomas de Chapultepec I Sección, Alcaldía Miguel Hidalgo, C.P. 11000, Cd. de México, México | | |
| | BMC Software Distribution de Mexico, S.A. de C.V. | Mercantile Folio 271309 | | | |
| 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 | | |

| Country | Group Member name | Registration number | Registered Office address | Contact email (common) | Expected categories of data transferred (common) |
|---|---|---|---|---|---|
| | BMC Software Limited Regional Headquarters Branch | 7054054189 | Al-Deghaither Center, Tahliyah Street, 11451 Riyad, Kingdom of Saudi Arabia | Privacy@bmc.com | Categories listed in Appendix 8 |
| South Africa | BMC Software Limited (Incorporated in England) - Branch entity | 1927903 | 2 Conference Lane Bridgewater One, Block 1, Bridgeway Precinct, Century City 7446 | | |
| Singapore | BMC Software Asia Pacific Pte Ltd | 199504342D | 600 North Bridge Road<br>#20-01/10 Parkview Square,<br>188778, Singapore | | |
| Taiwan | Taiwan 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 Software, Inc. | DE Charter # - 2165371 | 1209, Orange Street, c/o The Corporation Trust Company, Corporation Trust Center, 19801, Wilmington, Delaware, USA | | |
| | BMC Helix Federal, LLC | 10024034 | | | |

## APPENDIX 10 – LIST OF DEFINITIONS

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

**Applicable law** means the laws of the European country in which personal information was collected, unless otherwise specified.

**Binding Corporate Rules or "BCRs" or Policy** mean the personal information protection policies detailed in this document to ensure data protection and privacy compliance worldwide, especially with regard to international transfers of personal information between Group Members.

**BMC or BMC Software or Group Members** collectively mean the BMC Software entities bound by the Policy.

**Client** means a third party Controller or Processor on behalf and under the instructions of which BMC processes personal information, under the Policy and the applicable service agreement.

**Competent Supervisory Authority** means the supervisory authority competent for the data exporter.

**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.

**Exporter** means a Group Member based in Europe, and which transfers personal information to another Group Member based in a third country.

**Importer** means a Group Member based in a third country, and which gets transferred personal information from another Group Member based in Europe.

**European Economic Area or "EEA"** means the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway).

**Europe** means the EEA and Switzerland.

**GDPR** means Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended from time to time.

**Individual**, also designated as "data subject" under GDPR, means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Lead Supervisory Authority** means the Supervisory Authority who approved this Policy, which is the French "*Commission nationale de l'informatique et des libertés*" or "CNIL".

**Personal information,** also designated as “personal data” under GDPR, means any information relating to an identified or identifiable individual.

**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal information on behalf and under the instructions of a controller.

**Request for Disclosure** means a legally binding request from a public authority (e.g., a law enforcement authority or state security body), including judicial authorities, acting under the laws of a third country not recognized by the European Commission as ensuring an adequate level of protection and requesting the disclosure of personal information transferred pursuant to this Policy.

**Sensitive personal information** means personal 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, criminal convictions and offenses.

**Third country** means a country that is not a member of the EEA nor Switzerland.

# DOCUMENT INFORMATION

| | |
|---|---|
| **Version:** | 2.0 |
| **Last Modified on:** | 1 October 2026 |
| **Modified by:** | Maxime Roze, Chief Privacy Officer & Group Data Protection Officer |