The Controller and Processor Data Protection Binding Corporate Rules of BMC Software

04 August 2015

bmc

Table of Contents

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 and specifically to transfers of personal information between BMC group members ("**Group Members**") (a list of which is available at www.bmc.com).

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, whether to other Group Members or to external service providers, and 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.

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

The Policy will be published on the BMC Software, Inc. website accessible at www.bmc.com.

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 BMC collects and uses the personal information of its past, current and potential employees, customers, resellers, suppliers, service providers and other third parties, this activity, and the personal information in question, is covered and regulated by 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 also 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?

BMC must take proper steps to ensure that it uses 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.

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

[2] Personal information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in EU Directive 95/46/EC (available at http://eur-lex.europa.eu/).

BMC will apply the Policy globally, and in **all cases** where BMC processes personal information both manually and by automatic means when the personal information relates to past, current and potential employees, customers, resellers, suppliers, service providers and other third parties.

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.

- 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 Global Privacy Officer at the address below who will either deal with the matter or forward it to the appropriate person or department within BMC.

Jonathan Perez, Global Privacy Officer
Phone: +33 (0)1.57.00.63.81
Email: privacy@bmc.com
Address: Cœur Défense - Tour A, 10ème étage, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense Cedex

The Global Privacy Officer is responsible for ensuring that changes to the Policy are notified to the Group Members and to individuals whose personal information is processed by BMC. 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 European data protection 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

Rule 1 – 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 (e.g. in Europe, the local law implementing the EU Data Protection Directive 95/46/EC as amended or replaced from time to time) 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.

RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – BMC will explain to individuals, at the time their personal information is collected, how that information will be used.

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, including the following:

- the identification of the data controller and its contact details;
- information about an individual's rights to access and rectify their personal information;
- the uses and disclosures made of their personal information (including the secondary uses and disclosures of the information); and,
- the recipients or categories of recipients of their personal information.

This information will be provided when personal information is obtained by BMC from the individual or, if not practicable to do so at the point of collection, as soon as possible after that. BMC will follow this Rule 2A 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).

Rule 2B – BMC will only obtain and use personal information for those purposes which are known to the individual or which are within their expectations and are relevant to BMC.

Rule 1 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, legitimate purposes, and not use that personal information in a way which is incompatible with those purposes, BMC will honour 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) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

Rule 2C – BMC may only process personal information collected in Europe for a different or new purpose if BMC has a legitimate basis for doing so, consistent with the applicable law of the European country in which the personal information was collected.

If BMC collects personal information for a specific purpose in accordance with Rule 1 (as communicated to the individual via the relevant fair processing statement) 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 unless:

- it is within their expectations and they can express their concerns; 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 BMC is not satisfied that the processing is within the reasonable expectation of an individual, the individual's consent to the new uses or disclosures may be necessary.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – BMC will keep personal information accurate and up to date.

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.

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 not excessive.

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

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

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

BMC will implement appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, 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.

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, 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, and that they have in place appropriate technical and organizational security measures to safeguard personal information.

RULE 5 – HONORING INDIVIDUALS' RIGHTS

Rule 5A – BMC will adhere to the Subject Access Request 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 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 subject access in European data protection law. BMC will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) when dealing with requests from individuals for access to their personal information.

Rule 5B – BMC will deal with requests to delete, rectify or block inaccurate personal information or to cease processing personal information in accordance with the Subject Access Request Procedure.

Individuals are entitled to request rectification, deletion, blocking or completion, as appropriate of their personal information which is shown to be inaccurate or incomplete and, in certain circumstances, to object to the processing of their personal information. BMC will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

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

In principle, transborder transfers of personal information to third parties outside the BMC entities are not allowed without appropriate steps being taken, such as signing up to contractual clauses, which will protect the personal information being transferred.

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

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

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. BMC will assess whether sensitive personal information is required for the proposed use and when it is absolutely necessary in the context of the business.

Rule 7B – BMC will only use sensitive personal information collected in Europe where the individual's express 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 expressly agree to BMC collecting and using their sensitive personal information unless BMC is required to do so by local law or has another legitimate basis for doing so consistent with the applicable law of the country in which the personal information was collected. This permission to use sensitive personal information by BMC must be genuine and freely given.

RULE 8 – LEGITIMIZING DIRECT MARKETING

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

All individuals have the data protection right to object, free of charge, to the use of their personal information for direct marketing purposes and BMC will honor all such opt out requests.

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Where decisions are made by automated means, individuals will have the right to know the logic involved in the decision and BMC will take necessary measures to protect the 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 significantly affects them can

be based solely on the automated processing of personal information unless measures are taken to protect the legitimate interests of individuals.

- SECTION B: PRACTICAL COMMITMENTS

RULE 10 – COMPLIANCE

Rule 10 – BMC will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

BMC has appointed a Global Privacy 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 11 – TRAINING

Rule 11 – BMC will provide appropriate training to employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to process personal information in accordance with the Privacy Training Requirements attached as Appendix 3.

RULE 12 – AUDIT

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

RULE 13 – COMPLAINT HANDLING

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

RULE 14 – COOPERATION WITH DATA PROTECTION AUTHORITIES

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

RULE 15 – UPDATE OF THE POLICY

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

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

Rule 16A – BMC will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on its ability to comply with the Policy, BMC will promptly inform the Global Privacy Officer unless otherwise prohibited by a law enforcement authority.

Rule 16B – BMC will ensure that where there is a conflict between the legislation applicable to it and the Policy, the Core Privacy Team together with the legal department as appropriate will make a responsible decision on the action to take and will consult the data protection authority with competent jurisdiction in case of doubt.

- SECTION C: THIRD PARTY BENEFICIARY RIGHTS

European data protection law states that BMC's past, current and potential employees, customers, resellers, suppliers, service providers and other third parties whose personal information is collected and/or used in Europe by a Group Member acting as a controller (the "**Exporting Entity**") and transferred to a Group Member outside Europe (the "**Importing Entity**") must be able to benefit from certain rights to enforce any of the commitments in the Introduction to the Policy, Part II and the appendices in Part IV as follows:

- *Complaints*: Individuals may make a complaint to a European Group Member and/or to a European data protection authority in the jurisdiction of the Exporting Entity;

- *Proceedings*: Individuals may bring proceedings against an Exporting Entity in the courts of the jurisdiction of the Exporting Entity from which the personal information was transferred to enforce compliance by BMC with the Introduction to the Policy and Parts II and IV of the Policy; and/or

- *Liability*: Individuals may seek appropriate redress from an Exporting Entity including the remedy of any breach of the Introduction to the Policy and/or Parts II and IV of the Policy by any Importing Entity and, where appropriate receive

compensation from an Exporting Entity for any damage suffered as a result of a breach of the Introduction to the Policy, and/or Part II or IV of the Policy in accordance with the determination of a court or other competent authority.

- *Transparency*: Individuals also have the right to obtain a copy of the Policy and the intra-group agreement entered into by BMC in connection with the Policy.

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 an Importing Entity is not responsible for the breach, or that no such breach took place, will rest with the Exporting Entity which transferred the personal information to that Importing Entity under Part II of the Policy.

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 another Group Member, or 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 the Policy).

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

When BMC acts as a processor, BMC's European Clients 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 and so if BMC fails to comply with the terms of its contracts with its Clients, BMC's Clients may be in breach of applicable data protection law and BMC may face a claim for breach of contract which may result in the payment of compensation or other judicial remedies. In particular, 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 when there is a specific obligation falling on BMC to comply with the Policy in the contract it has with that Client. 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.

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 European data protection 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

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 a controller 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 as required under 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, complying with instructions from its Clients, as required under the terms of its contracts with its Client, in order to assist them to meet the individual Client's obligation to keep personal information accurate and up to date.

RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – BMC will assist a controller to comply with the requirement to explain to individuals how that information will be used to the extent reasonably possible.

BMC's 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.

BMC will provide such assistance and information to its Clients as may be required under the terms of its contracts with its Clients to comply with this requirement. For example, BMC

may be required to provide information about any sub-processors appointed by BMC to process Client personal information on its behalf under the terms of a contract with a particular Client.

Rule 2B – BMC will only use personal information on behalf of and in accordance with the instructions of the controller.

BMC will only use personal information in compliance with the terms of a contract it has with a Client.

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.

In such circumstances, BMC will act in accordance with the instructions of that Client and return, destroy or store the personal information, including any copies of the personal information, in a secure manner or as otherwise required in accordance with the terms of its contract with that Client.

In the event that legislation prevents BMC from returning the personal information to a Client or destroying it, BMC will maintain the confidentiality of the personal information and will not process the personal information otherwise than in accordance with the terms of its contract with that Client.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3 – BMC will assist controllers to keep the personal information accurate and up to date.

BMC will comply with any instructions from a Client, as required 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 will delete, anonymise, update or correct 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 controllers 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 reasonably necessary measures to enable its Clients to comply with their duty to respect the rights of individuals. In particular, if any Group Member receives a subject access request, the Group Member 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 a controller.

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 controls the security and organizational measures required to safeguard that information consistent with the law of the European country applicable to the Client.

Rule 5B – BMC will notify a controller of any security breach in accordance with the terms of a contract with a controller.

Group Members will notify a Client of any security 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 Group Member's contract with that Client.

Rule 5C – BMC will comply with the requirements of a controller 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 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 so that their general consent is obtained. If, on reviewing this information, a Client objects to the appointment of a sub-processor to process personal information on its behalf, that Client will be entitled to take such steps as are consistent with the terms of its contract with BMC and as referred to in Rule 2B of Part III of this Policy.

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

Group Members 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 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 Group Member's contract with 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 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; 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.

- 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 Global Privacy 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 ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under Part III of the Policy, BMC will promptly inform:

- **the controller, as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority);**
- **BMC's Global Privacy Officer and the Vice President, EMEA General Counsel; and**
- **The appropriate data protection authority competent for the controller.**

Rule 12B – BMC will ensure that where it receives a legally binding request for disclosure of personal information which is subject to Part III of the Policy, BMC will:

- **notify the controller promptly, unless prohibited from doing so by a law enforcement authority or agency; and**
- **put the request on hold and notify the lead data protection authority who approved this Policy (i.e. the CNIL) and the appropriate data protection authority competent for the controller unless prohibited from doing so by a law enforcement authority or agency. In such case, BMC will use its best efforts to inform the requesting authority or agency about its obligations under European data protection law and to obtain the right to waive this prohibition. Where such prohibition cannot be waived, despite BMC's efforts, BMC will provide the competent data protection authorities with an annual report providing general information about any requests for disclosure it may have received from the requesting authority or agency, to the extent that BMC has been authorized by said authority or agency to disclose such information.**

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

European data protection law states that individuals whose personal information is processed in Europe must be given rights to enforce the Policy as third party beneficiaries where they cannot bring a claim against a controller in respect of a breach of any of the commitments in the Introduction to the Policy, Part III or the appendices in Part IV of the Policy (as applicable) by a Group Member (or by a sub-processor) acting as a processor because the controller has factually disappeared, or ceased to exist in law, or has become insolvent and no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law. As a result, BMC's past, current and potential employees, customers, resellers, suppliers, service providers and other third parties whose personal information is processed in Europe by a Group Member acting as a processor (the "Exporting Entity") and/or transferred to a Group Member outside Europe (the "Importing Entity") benefit from certain rights to enforce the Introduction to the Policy, Part III and the appendices in Part IV of the Policy (as applicable) as follows:

- Where personal information is transferred under Part III of the Policy and where:

  (i) the individual whose personal information is transferred is unable to bring a claim against the data controller in respect of a breach of the Introduction to the Policy, Part III of the Policy or the appendices in Part IV of the Policy (as applicable) by a Group Member (or by a sub-processor) acting as a processor because the data controller has factually disappeared or ceased to exist in law or has become insolvent; and

  (ii) no successor entity has assumed the entire legal obligations of the data controller by contract or by operation of law,

that individual will have the following third party beneficiary rights;

(a) *Enforcement of compliance*: to seek enforcement of compliance with the Introduction to the Policy, Part III of the Policy and the appendices in Part IV of the Policy (as applicable);

(b) *Complaints*: to make a complaint to a European data protection authority in the jurisdiction of the Exporting Entity, or where there is no Exporting Entity, in the jurisdiction from which the personal information is transferred and/or to a Group Member in Europe (such complaints to be dealt with in accordance with the Complaint Handling Procedure set out in Appendix 5);

(c) *Liability*: to bring proceedings against:

(i) the Exporting Entity in the courts of the jurisdiction of the Exporting Entity from which the personal information was transferred (in which case the Exporting Entity will accept liability as if that entity had committed the breach in question in the European Member State in which that Exporting Entity is established); or

(ii) where there is no Exporting Entity, the Importing Entity in the jurisdiction of the European Member State where the individual resides;

(d) *Compensation*: where appropriate, to receive compensation from the Exporting Entity or, where there is no Exporting Entity, the Importing Entity as appropriate for any damage suffered as a result of a breach of the Introduction to the Policy, Part III of the Policy or the appendices in Part IV of the Policy (as applicable) by:

(i) an Importing Entity; or

(ii) by any third party data processor which is established outside Europe and which is acting on behalf of an Importing Entity or an Exporting Entity

in accordance with the determination of the court or other competent authority;

(e) *Transparency:* to obtain a copy of the Policy and the intra-group agreement.

- Where a Group Member outside Europe is acting as a processor on behalf of a third party controller, in the event that an individual suffers 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, Part III of the Policy or the appendices in Part IV of the Policy (as applicable), the burden of proof to show that an Importing Entity 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 the Exporting Entity, or where there is no Exporting Entity, with the Importing Entity.

- The Exporting Entity or, where there is no Exporting Entity, the Importing Entity will ensure that any action necessary is taken to remedy any breach of the Introduction to the Policy, Part III of the

Policy or the appendices in Part IV of the Policy (as applicable) by an Importing Entity or any third party processor which is established outside Europe and which is processing personal information on behalf of a data controller.

PART IV: APPENDICES

APPENDIX 1

SUBJECT ACCESS REQUEST 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 meeting the requirements of data protection law.

1.2 When BMC acts as a controller, individuals whose personal information is collected and/or used in Europe[3] have the right to be informed by BMC whether any personal information about them is being processed by BMC. This is known as the right of subject access.

1.3 In addition, all individuals whose personal information is collected and/or used in Europe by BMC acting as controller, and transferred between BMC group members ("**Group Members**") will also benefit from the right of subject access and such subject access requests will be dealt with in accordance with the terms of this Subject Access Request Procedure ("**Procedure**").

1.4 This Procedure explains how BMC deals with a subject access request relating to personal information which falls into the categories in sections 1.2 and 1.3 above (referred to as "**valid request**" in this Procedure).

1.5 Where a subject access request is subject to European data protection law because it is made in respect of personal information collected and/or used in Europe, such a request will be dealt with by BMC in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.

2. Individuals' rights

2.1 An individual making a valid request to BMC when BMC is a controller of the personal information requested is entitled to:

2.1.1 Be informed whether BMC holds and is processing personal information about that person;

[3] In this Procedure Europe means the EEA plus Switzerland

2.1.2 Be given a description of the personal information, the purposes for which they are being held and processed and the recipients or classes of recipient to whom the information is, or may be, disclosed by BMC; and

2.1.3 Communication in intelligible form of the personal information held by BMC.

2.2 The request must be made in writing (where required), which can include email.[4]

2.3 BMC must respond to a valid request within 40 calendar days (or any shorter period as may be stipulated under local law) of receipt of that request.

2.4 BMC is not obliged to comply with a subject access request unless BMC is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request and to locate the information which that person seeks.

3. Process

3.1 Receipt of a subject access request when BMC is a controller of the personal information requested

3.1.1 If BMC receives any request from an individual for their personal information, this must be passed to the Global Privacy Officer at privacy@bmc.com immediately upon receipt indicating the date on which it was received together with any other information which may assist the Global Privacy Officer to deal with the request.

3.1.2 The request does not have to be official or mention data protection law to qualify as a subject access request.

3.2 Initial steps

3.2.1 The Global Privacy Officer will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

3.2.2 The Global Privacy Officer will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

[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.

4. Exemptions to the right of subject access for requests made to BMC as a controller

4.1 A valid request may be refused on the following grounds:

4.1.1 Where the subject access request is made to a European Group Member and relates to the use or collection of personal information by that Group Member, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located; or

4.1.2 Where the subject access request does not fall within section 4.1.1 because it is made to a non-European Group Member and:

(a) if, in the opinion of BMC, compliance with a subject access request would: (i) prejudice the essential business interests of BMC (which includes management planning, management forecasting, corporate finance or negotiations with a data subject); (ii) it is necessary to do so to safeguard national or public security, defence, the prevention, investigation, detection and prosecution of criminal offences; or (iii) for the protection of the data subject or of the rights and freedoms of others; or

(b) if the personal information is held by BMC in non-automated form and is not or will not become part of a filing system; or

(c) where the personal information does not originate from Europe and the provision of the personal information requires BMC to use disproportionate effort.

4.1.3 The Global Privacy Officer will assess each request individually to determine whether any of the above-mentioned exemptions applies.

5. BMC's search and the response

5.1 The Global Privacy Officer together with the Global Security Services Director will arrange a search of all relevant electronic and paper filing systems.

5.2 The Global Privacy Officer may refer any complex cases to the Vice President EMEA General Counsel for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

5.3 The information requested will be collated by the Global Privacy Officer into a readily understandable format (internal codes or identification numbers used at BMC that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Global Privacy Officer which includes information required to be provided in response to a subject access request.

5.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in section 2.1 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

6. Subject access requests made to BMC where BMC is a processor of the personal information requested

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

6.2 Certain data protection obligations are passed to BMC in the contracts BMC has with its clients and BMC must act in accordance with the instructions of its clients and undertake any reasonably necessary measures to enable its clients to comply with their duty to respect the rights of individuals. This means that if any Group Member receives a subject access request in its capacity as a processor for a client, that Group Member must transfer such request promptly to the relevant client and not respond to the request unless authorized by the client to do so.

7. Requests for erasure, amendment or cessation of processing of personal information

7.1 If a request is received for the erasure, amendment, or cessation of processing of an individual's personal information where BMC is the controller for that personal information, such a request must be considered and dealt with as appropriate by the local legal and compliance officer.

7.2 If a request is received advising of a change in an individual's personal information where BMC is the controller for that personal information, such

information must be rectified or updated accordingly if BMC is satisfied that there is a legitimate basis for doing so.

7.3 When BMC deletes, anonymises, updates, or corrects personal information, either in its capacity as controller or on instruction of a client when it is acting as a processor, BMC will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

7.4 If the request made to BMC as a controller is to cease processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by BMC, or on the basis of other compelling legitimate grounds, the matter will be referred to the Global Privacy Officer to assess. Where the processing undertaken by BMC is required by law, the request will not be regarded as valid.

7.5 All queries relating to this Procedure are to be addressed to the Global Privacy Officer.

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

- Ensuring that the Policy and other privacy related policies, objectives and standards are defined and communicated.
- Providing clear and visible senior management support and resources for the Policy and for privacy objectives and initiatives in general.
- Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Policy, strategic plans, business objectives and regulatory requirements.
- Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.
- Ensuring that BMC's business objectives align with the Policy and related privacy and information protection strategies, policies and practices.
- Facilitating communications on the Policy and privacy topics with the BMC Executive Leadership Team and Board of Directors.
- 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. Project Working Group

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

The Project Working Group is responsible for:

- Promoting the Policy at all levels in their organizations.
- Facilitating in-depth reviews of business processes for assessing compliance with the Policy as necessary.
- Ensuring that BMC's business objectives align with the Policy and related privacy and information protection strategies, policies and practices.
- Assisting the Core Privacy Team in identifying, evaluating, prioritizing, and driving remedial actions consistent with BMC's policies and regulatory requirements.
- Implementing decisions made by the Executive Steering Committee within BMC on a global scale.

3. Core Privacy Team

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

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:

- Responding to inquiries and complaints relating to the Policy from employees, customers and other third parties, 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.

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

- Providing input on audits of the Policy, coordinating responses to audit findings and responding to inquiries of the data protection authorities.

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

- Promoting the Policy and privacy awareness across business units and functional areas through privacy communications and training.

- Evaluating privacy processes and procedures to ensure that they are sustainable and effective.

- Reporting periodically on the status of the Policy to the Executive Steering Committee.

- Hosting and coordinating meetings of the Project Working Group.

- 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.

- Escalating issues relating to the Policy to the Project Working Group and Executive Steering Group where required.

- 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 compliance officers

BMC has appointed a number of local compliance officers to assist with the operation of the Policy at country level. The role of the local compliance officers is to:

- Assist the Core Privacy Team with the implementation and management of the Policy in their jurisdiction.

- 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 has overall responsibility for compliance and ethics training within BMC, including the delivery and tracking 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 subject access requests from individuals 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 BMC's training on the Policy will cover the following main areas and employees receive training appropriate to their roles and responsibilities within BMC:

4.1.1 Background and rationale:

(a) What is data protection law?

(b) How data protection law will affect BMC internationally

(c) The scope of the Policy

(d) Terminology and concepts

4.1.2 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

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

(a) Subject Access Request Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

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 the data protection authorities in the European Member States from which the personal information is transferred. One of the requirements of the data protection authorities 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 data protection authorities, 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 Global Privacy 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 processor, audits of compliance with the commitments made in Part III of the Policy may also be carried out by or on behalf of BMC's clients in accordance with the terms of a contract BMC has with a client in respect of such processing, and such audits may also extend to any sub-processors 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 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** and BMC may utilize other accredited internal/external auditors as determined by BMC.

2.3.2 In the event that a third party controller on whose behalf BMC processes personal information exercises their right to audit BMC for compliance with Part 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**, the **Executive Steering Committee** and other appropriate management personnel. The Assurance Department will also provide a summary of the audit results to the **Audit Committee**, which reports directly to the Board.

2.4.2 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, BMC has agreed to:

(a) provide copies of the results of any audit of the Policy to a European data protection authority of competent jurisdiction; 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.

2.4.3 BMC's Global Privacy Officer will be responsible for liaising with the European data protection authorities for the purpose of providing the information outlined in section 2.4.2.

2.4.4 In addition BMC has agreed that European data protection authorities may audit Group Members for the purpose of reviewing compliance with the Policy in accordance with the terms of The Controller and Processor Data Protection Binding Corporate Rules of BMC Software Cooperation Procedure.

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 transferred between the BMC group members ("**Group Members**"). The content of the Policy is determined by the data protection 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 Global Privacy Officer or by emailing privacy@bmc.com. 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 Global Privacy 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 Global Privacy Officer will liaise with colleagues from 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 Global Privacy Officer will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, BMC's Global Privacy Officer will advise the complainant accordingly and provide a reasonable estimate (not exceeding six 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 Global Privacy Officer (or the individual or department within BMC tasked by the Global Privacy Officer with resolving the complaint) or any aspect of a finding, and notifies the Global Privacy 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 collected and/or used and in accordance with European data protection law also have the right to complain to a European data protection authority and/or to lodge a claim with a court of competent jurisdiction whether or not they have first made a complaint to BMC.

3.1.5 The jurisdiction from which the personal information was transferred will determine to which data protection authority a complaint may be made.

3.1.6 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 in Europe responsible for exporting the personal information.

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 When a client ceases to exist

In circumstances where a client has disappeared, no longer exists or has become insolvent, individuals whose personal information is collected and/or used in accordance with European data protection law and transferred between Group Members on behalf of that client have the right to complain to BMC and 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 a European data protection 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] data protection 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 European data protection authority in relation to the Policy.

2.2 BMC will actively review and consider:

2.2.1 any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Policy; and

2.2.2 the views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules for data controllers and Binding Corporate Rules for data processors.

2.3 Subject to applicable law and respect for the confidentiality and trade secrets of the information provided, BMC will provide upon request copies of the results of any audit of the Policy to a relevant European data protection authority.

2.4 BMC agrees that:

2.4.1 where any BMC group member ("**Group Member**") is located within the jurisdiction of a data protection authority based in Europe, BMC agrees that that data protection 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 the case of a Group Member located outside Europe, BMC agrees that a data protection 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) on giving reasonable prior notice and during business hours,

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

with full respect to the confidentiality of the information obtained and to the trade secrets of BMC (unless this requirement is in conflict with local applicable law).

2.5 BMC agrees to abide by a formal decision of the applicable data protection authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policy.

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] data protection 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 as soon as is reasonably practical to the Commission nationale de l'informatique et des libertés ("**CNIL**") and to any other relevant European data protection authorities.

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. If such change is contrary to any term of the contract between BMC and that client, BMC will communicate the proposed change before it is implemented, and with sufficient notice to enable affected clients to object. BMC's Client may then suspend the transfer of personal information to BMC and/or terminate the contract, in accordance with the terms of its contract with BMC.

3. Administrative changes to the 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 European data protection authorities at least once a year. BMC will also provide a brief explanation to the CNIL and to any other relevant data protection authorities of the reasons for any notified changes to the 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

[6] References to Europe for the purposes of this document includes the EEA and Switzerland

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 Global Privacy 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:

4.2.1 to the Group Members bound by the Policy via the BMC Intranet; and

4.2.2 systematically to clients on whose behalf BMC processes personal information and data subjects who benefit from the Policy via bmc.com.

4.3 BMC's Global Privacy 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

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

Document Information

Version:	1.0
Created by:	Jonathan Perez
Last Modified on:	4 August 2015
Modified by:	Joshua Stratmann

BMC delivers software solutions that help IT transform digital enterprises for the ultimate competitive business advantage. From mainframe to cloud to mobile, we pair high-speed digital innovation with robust IT industrialization—allowing our customers to provide amazing user experiences with optimized IT performance, cost, compliance, and productivity. We believe:

- **Technology is the heart of every business**
- **IT drives business to the digital age**

BMC – Bring IT to Life.