Bristol-Myers Squibb

Binding Corporate Rules (BCRs) for intra-group transfers of personal data to non EEA countries
SUMMARY

1. INTRODUCTION

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES
   2.1. DEFINITIONS
   2.2. DATA PROTECTION PRINCIPLES

3. SCOPE OF THE BCRS
   3.1. GEOGRAPHICAL SCOPE
   3.2. MATERIAL SCOPE

4. EFFECTIVENESS OF THE BCRS
   4.1. TRANSPARENCY AND INFORMATION RIGHT
   4.2. RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA
   4.3. AUTOMATED INDIVIDUAL DECISIONS
   4.4. INTERNAL COMPLAINT MECHANISM
   4.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS
        THAT ARE MEMBERS OF THE GROUP
   4.6. TRAINING PROGRAMS
   4.7. AUDIT PROGRAMME

5. BINDING NATURE OF THE BCRS
   5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE
   5.2. THIRD PARTY BENEFICIARY RIGHTS
   5.3. LIABILITY
   5.4. SANCTION
   5.5. MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION
        AUTHORITIES

6. FINAL PROVISIONS
   6.1. RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs
   6.2. RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL
        PROCESSORS AND CONTROLLERS
   6.3. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF
        BCRs
   6.4. UPDATES OF THE BCRs
   6.5. DEROGATIONS OF ARTICLE 26 EU DIRECTIVE 95/46
6.6 APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

APPENDIXES
1. INTRODUCTION

Bristol-Myers Squibb (BMS) has decided to commit its Group in a process for the adoption of Binding Corporate Rules (BCRs), which will aim to regulate intra-group data transfers from EEA countries to non EEA countries.

This decision is a full part of the proactive policy with regard to Data Privacy that Bristol-Myers Squibb has followed for several years. To date, BMS has an internal organization which integrates Data Protection Principles in its whole decision making process, in accordance with the provisions of the 95/46 and 2002/58 EU Directives. This organization singularizes itself through the existence, at a worldwide level, of a "Privacy Council" both in connection with BMS Company and with a network of "Data Privacy Officers" responsible for enforcing, at local level, all defined guidelines, policies and procedures relating to Data Protection Issues. The importance of Privacy and Confidentiality Principles is also highlighted in our Standards of Business Conduct and Ethics.

In the normal course of business, BMS receives, collects, maintains and uses significant amounts of personal data from individuals. Some of these data may include sensitive information that may pertain to a person's health. BMS and its employees are responsible for protecting and respecting personal information to which they have access. Therefore, we believe that our BCRs are an essential tool to effectively manage this important responsibility.

In this context, the decision to adopt BCRs is one step further toward a full commitment to Data Protection compliance. Beyond providing adequate protection for the transfer of personal data outside the EEA, this approach aims to optimize the broadcasting and sharing of our culture on Privacy within our Group in order to enhance this commitment to all of our stakeholders, partners and/or interlocutors.

With regard to the scope of our BCRs, appropriate entities and employees of the BMS Group shall comply with the following guidelines, as well as with applicable local laws.

Bristol-Myers Squibb EMEA, a subsidiary company located in Rueil-Malmaison, France, is in charge of implementing, in coordination with the headquarters located in the United States, all the data protection policies and procedures available within the Group at European level.

For many years, the Legal Privacy Counsel EU has developed a privacy practice and is the best placed to enforce the BCRs within the Group. Thus, the Head Controller has appointed the Legal Privacy Counsel EU and the Global Privacy Office for supervising, at global level, the implementation of the BCRs in all appropriate BMS entities. Therefore, we have asked the French Data Protection Authority (the CNIL) to review our BCRs as the coordinating Authority within the European scheme of cooperation for BCRs’ approval, in accordance with G29 Working Party 133 Working Paper dated January, 10, 2007.

At local level, and according to the terms of our BCRs, each Local Data Controller will have to sign the BCRs and shall take every necessary step to ensure compliance with the provisions of the BCRs. Compliance with these guidelines and procedures will especially rely on training programs and auditing activities, on a day to day basis.

Would a violation of the BCRs be established, any corrective measure (legal, technical or organizational measure) as well as any appropriate sanction (against the local Data Controller
or, according to local labor law, a local employee) may be taken on the initiative of the Head Controller, the Privacy Council, the Global Privacy Office, the Legal Privacy Counsel EU, the Office of Compliance and Ethics, the local Data Controller or the local Data Privacy Officer.

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs are defined in appendix 1, provided that these terms and expressions shall always be interpreted according to the EU 95/46 and 2002/58 Directives.

2.2. DATA PROTECTION PRINCIPLES

Within the scope of the BCRs (see paragraph 3), any transfer of personal data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, defined in specific paragraphs of the BCRs or in appendix 2, in accordance with the provisions of the EU 95/46 and 2002/58.

- **Legal basis for processing personal data and sensitive personal data**: personal data and sensitive personal data shall only be processed under the conditions defined in the 95/46 EU Directive.

- **Purpose limitation**: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

- **Data quality and proportionality**: personal data shall be processed fairly and lawfully. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Personal data shall be accurate and, where necessary, kept up to date. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

- **Automated individual decisions**: each data subject has the right not to be subject to a decision which produces legal effects concerning him and which would be based solely on automated processing of data.

- **Information right**: personal data shall always be collected and further processed on a transparent basis (see paragraph 4.1)

- **Rights of access, rectification, erasure and blocking of data**: data subjects are entitled to be told what information BMS holds on them and to keep this information under control (see paragraph 4.2).

- **Security and confidentiality**: appropriate technical and organizational measures shall be implemented to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing (see paragraph 4.5).
3. SCOPE OF THE BCRs

3.1 GEOGRAPHICAL SCOPE

The BCRs apply to personal data processed within the EEA and transferred outside the EEA. Appendix 3 gives a list of all BMS entities bound by the BCRs.

3.2 MATERIAL SCOPE

The nature and purposes of the personal data being transferred within the scope of the BCRs is detailed in appendix 4.

4. EFFECTIVENESS OF THE BCRs

4.1 TRANSPARENCY AND INFORMATION RIGHT

To make the data processing fair, personal data shall always be collected and further processed on a transparent basis. Thus:

1. The BCRs shall always be readily available to every data subject and therefore shall be uploaded both on BMS intranet and internet corporate website. Furthermore, a data subject will always be able to obtain, upon request, a copy of the BCRs from the local Data Privacy Officer, the local data controller, the Legal Privacy Counsel EU or the Global Privacy Office.

2. All data processing and, when appropriate, data transfers outside the EEA, shall be associated with relevant data protection notices.

Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall be able to provide templates of notices to every local data controller within the Group, for any purpose that requires information to be made to the data subjects.

BMS will provide a data subject with at least the following information, except where he already has it:

a) the identity of the controller and of his representative, if any, and, when appropriate, the place in which the Local Data Importer is based outside the EEA;

b) the purposes of the processing for which the data are intended, and, when appropriate, the purpose(s) of the transfer(s) outside the EEA;

c) any further information such as:

- the categories of data concerned;
- the recipients or categories of recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data concerning him.
Where, with regard to an existing data processing, a new purpose or a new category of recipient arise, the appropriate notice of information shall be consequently modified and the data subjects shall be informed.

Where the data has not been directly obtained from the data subjects, BMS will provide with the information above at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

According to article 11.2 of the 95/46 EU Directive, information will exceptionally not apply where the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law (see paragraph 6.3).

4.2 RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA

Data subjects are entitled to be told what information BMS holds on them and to keep this information under control. Thus:

1. Every data subject has the right to obtain from BMS:

a) without constraint at reasonable intervals and without excessive delay or expense:

   - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

   - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

b) as appropriate the rectification, erasure or blocking of personal data, in particular because of the incomplete or inaccurate nature of the data;

c) to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him

According to the 95/46 EU directive, the exercise of those rights may be subject to certain limitations.

2. Every data subject shall be clearly informed, in accordance with paragraph 4.1, on how he can exercise his rights.

3. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure the exercise of the rights specified above. In particular, all BMS employees shall be trained to recognize a data subject access, rectification, erasure or blocking request. Each request shall be acknowledged and handled according to the local procedure in place. A specific answer, given within a reasonable period of time, shall be systematically given to the data subject. If the request is found legitimate, BMS shall take any necessary step to handle the matter in due times. If the request is denied, the reason for denial shall be communicated in writing to the data subject. In such a case, the data subject may follow the internal complaint mechanism specified in paragraph 4.4.
4. Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall always be at the disposal of both local data controllers and data subjects to provide any help.

4.3 AUTOMATED INDIVIDUAL DECISIONS

Subject to local applicable law, every data subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, reliability, conduct, etc.

4.4 INTERNAL COMPLAINT MECHANISM

If a data subject believes that its personal data is not processed in accordance with the BCRs or the applicable local law, he may register a claim with BMS to obtain adequate correction measures and, where appropriate, adequate compensation (see paragraph 5.2 and 5.3). Therefore:

1. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure a complaint mechanism to be consistent and to ensure sufficient information to be provided to the data subjects about these procedures. The complaints shall be dealt, according to each category of data subjects involved (i.e. employees, healthcare professionals, etc.), by a clearly identified local department or by the local Data Protection Officer. The ones in charge of handling a claim shall benefit from an appropriate level of independence in the exercise of their duties. When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (three months).

2. If the data subject or BMS representatives fail to solve the claim at local level, the complaint handling mechanism shall allow to escalate the problem, within a reasonable period of time (three months), to the Office of Compliance and Ethics, the Legal Privacy Counsel EU or the Global Privacy Office.

3. Each local data controller and local data privacy officer shall regularly report to the Legal Privacy Counsel EU and the Global Privacy Office about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Privacy compliance.

4. All BMS representatives and employees shall, at local level, do their best efforts to help the local data controller or the local data privacy officer to settle a complaint.

Difficulties met by a data subject shall be referred to the relevant court or other Public Authority only if the internal complaint mechanism fails, in a reasonable period of time, to settle a claim (see paragraph 5.3).
4.5 SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

Ensuring that personal information is appropriately protected from data breaches is a BMS top priority. Thus:

1. Each local data controller shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Consequently, appropriate information security policies and procedures shall be designed and implemented within the Group. These security policies set up all appropriate physical and logical measures with a view to prevent or deter accidental destruction, modification or unauthorized disclosure or access to personal data. These policies and procedures shall be regularly audited (see paragraph 4.7).

2. Sensitive Data shall be processed with enhanced and specific security measures.

3. Access to Personal Data is limited to recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may occur if a BMS employee fails to comply with the appropriate information security policies and procedures.

Where a local data controller requests that another BMS entity undertakes processing of personal data on its behalf, the following safeguards shall be followed:

1. Where the data processing is carried out, the local data controller shall choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures. The appointed BMS entity shall undertake in writing to provide those sufficient guarantees. Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall be able to provide templates of the appropriate clauses to a local data controller within the Group.

2. The appointed entity must not process the data except on instructions from the controller, unless he is required to do so by law.

3. Upon termination of the work to be done, the appointed entity shall undertake to delete all the data transferred or, if any legal data retention requirement is applicable, to keep it recorded, provided that appropriate technical and organizational measures are taken to protect personal data against any unlawful form of processing.
4.6 TRAINING PROGRAMS

All BMS employees shall be provided with specific training programs in order to improve their practical skills and knowledge that relate to data protection issues, especially the BCRs. Thus, privacy training programs are full part of everyone's professional development within BMS Group:

1. BCR's and all related guidelines, procedures or policies shall be uploaded on BMS corporate intranet and permanently accessible to every BMS employee.

2. Access to the BCRs and all related guidelines, procedures or policies shall be granted to every BMS new employee. Internal notices shall also be transmitted within the Group to raise awareness on the BCRs.

3. New employees shall be required to follow a privacy compliance training program. Furthermore, all employees shall be required to follow such a program, on a regular basis. All employees must pass a knowledge check (certification) following their completion of the training to confirm their knowledge and skills on privacy issues.

4. Those who collect, process or have access to personal data may benefit from additional specific focused training programs (i.e. training related to HR personal data, health data, etc.).

5. At local level, each data controller and/or data privacy officer shall feel free to enhance the privacy training programs described above by adding any appropriate training material.

6. Privacy training programs shall be reviewed and approved by experienced BMS officers, in coordination with the local data privacy officers, the Legal Privacy Counsel EU and the Global Privacy Office. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.7).

4.7 AUDIT PROGRAMME

Data Protection audits shall be carried out on a regular basis (at least one audit every 3 years) by internal or external accredited audit teams to ensure that the BCRs and all related policies, procedures or guidelines are updated and applied:

1. Data Protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place. However, the scope of each audit can be strengthened to limited aspects of the BCRs and/or the related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place.

2. Data Protection audits shall be decided directly by the Compliance / Audit Departments or upon specific request of the Head Controller, the Office of Compliance and Ethics, a local data controller, a local data privacy officer, the Legal Privacy Counsel EU or the Global Privacy Office. The ones in charge of handling an audit will always benefit from an appropriate level of independence in the exercise of their duties.
3. The results of all audits shall be communicated to the Global Privacy Council and/or the Legal Privacy Counsel EU and/or the Global Privacy Office and/or the local privacy officer and/or the local data controller.

4. The relevant Data Protection Authorities shall receive a copy of such audit upon request. Each local data controller shall accept to be audited by a Data Protection Authority and to abide by the advice of a Data Protection Authority on any issue related to the BCRs.

5. As provided by section 3 of paragraph 5.1 below, Local data privacy officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall report every year to the Head controller about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of personal data processing implemented, management of complaints, etc.). Furthermore, each local data privacy officer shall take every necessary step to make sure that local data controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check list" shall be used at local level to make compliance checks.

6. The Legal Privacy Counsel EU shall also regularly report to the Head Controller and the Privacy Council about the implementation of the BCRs within each local Data Controller.

7. Thanks to the audit results and the reports mentioned above, the Head Controller and/or the Privacy Council and/or the Global Privacy Office shall decide any appropriate legal, technical or organizational measure in order to improve Data Protection management within the Group, both at global and/or local level.

5. BINDING NATURE OF THE BCRs

5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE

BMS has an internal organization which integrates the Data Protection Principles in its whole decision making process.

This organization singularizes itself through the existence, at a worldwide level, of a "Privacy Council" in connection both with the Head Controller and with a network of "Data Privacy Officers" responsible for enforcing, at local level, all defined guidelines, policies and procedures relating to data protection issues.

Compliance with those guidelines and procedures rely on training programs and auditing activities for all our employees, on a day to day basis. The importance of Privacy and Confidentiality Principles is also highlighted in our Code of business conduct and Ethics.

The Head Controller has appointed the Legal Privacy Counsel EU and the Global Privacy Office for supervising, at global level, the implementation of the BCRs in all the appropriate BMS entities.

At local level, each local data protection officer shall be responsible for the implementation of the BCRs. Thus:
1. Each entity shall take every necessary step to make sure that local data controllers comply with the provisions of the BCRs. To this end, a 'BCR compliance check list' shall be used at local level to make compliance checks. Data Protection audits decided by the Compliance / Audit Departments, the Legal Privacy Counsel EU or the Global Privacy Office may focus on how these compliance checks are made at local level.

2. Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall always be at the disposal of both local data controller and data subjects to provide any help with regard to a data protection issue, especially the BCRs.

3. The local data privacy officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall report every year to the Head controller about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of personal data processing implemented, management of complaints, etc.), especially the implementation of the BCRs.

4. Each local data controller and local data privacy officer shall regularly report to the Legal Privacy Counsel EU and the Global Privacy Office about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Privacy.

5. Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall be able to provide any appropriate templates (i.e. notices of information, clauses, etc.) to each local data controller within the Group for any purpose related to a data protection issue.

Furthermore, in terms of supervision of compliance, specific measures shall be taken to ensure the right implementation of the BCRs:

1. The Legal Privacy Counsel EU and the Global Privacy Office shall regularly report to the Head Controller and the Privacy Council about the implementation of the BCRs within each local Data Controller.

2. Data Protection audits shall be decided directly by the Compliance / Audit Departments or upon specific request of a local data privacy officer, the Office of Compliance and Ethics, the Legal Privacy Counsel EU or the Global Privacy Office. The results of all audits or reports shall be communicated to the Global Privacy Council and/or the Legal Privacy Counsel EU and/or the Global Privacy Office.

3. Thanks to the audit results and the reports mentioned above, the Head Controller, the Office of Compliance and Ethics, the Privacy Council, the Global Privacy Office, the Legal Privacy Counsel EU, a local data controller or a local data privacy officer shall decide any appropriate measure in order to improve Data Protection management within the Group, both at global and/or local level.

4. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the local Data Controller or, according to local labour law, a local employee) may be taken on the initiative of the Head Controller, the Privacy Council, the Global Privacy Office, the Legal Privacy Counsel EU, a
local Data Controller or a local Data Privacy Officer, in coordination with the Office of Compliance and Ethics.

5. Privacy training programs shall be reviewed and approved by BMS senior officers, in coordination with the Global Privacy Office, the Legal Privacy Counsel EU and local data privacy officers. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.7).

5.2 THIRD PARTY BENEFICIARY RIGHTS

A data subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs. Thus:

1. Each Data Subject shall have the right to take its case, at its best convenience, to the competent Data Protection Authorities or before the jurisdiction of the Local Data Exporter or before the jurisdiction of the Local Data Importer, for any breach of the BCRs.

2. According to the relevant provisions in paragraph 5.3, each Data Subject who has suffered damage shall be entitled to receive compensation (eg. judicial remedies), provided that the internal complaint mechanism failed to settle the case (see paragraph 4.4).

3. The BCRs shall always be readily available to every data subject, in the conditions described in paragraph 4.1. Furthermore, a data subject shall always be able to obtain, upon request, a copy of the BCRs from the local Data Protection Officer, the local data controller, the Legal Privacy Counsel EU or the Global Privacy Office.

5.3 LIABILITY

Either the Local Data Importer or the Local Data Exporter shall be liable for any breach of the BCRs, under the following conditions:

1. In cases involving allegations of breach by the Local Data Importer, the data subject shall first request the Local Data Exporter to take appropriate action to enforce his rights against the Local Data Importer. If the Local Data Exporter does not take such action within a reasonable period (which under normal circumstances would be three months), the data subject may then enforce his rights against the Local Data Importer directly. A data subject shall also be entitled to proceed directly against a Local Data Exporter that has failed to use reasonable efforts to determine that the Local Data Importer is able to satisfy its obligations under the BCRs. Both Local Data Exporter and Local Data Importer shall agree to take necessary actions to remedy and to pay compensation for actual damages they may be recognized liable for. Both Local Data Exporter and Local Data Importer shall therefore have sufficient financial resources at their disposal to cover the payment of compensation for breach of the BCRs. Liability as between the parties shall be limited to actual damage suffered. Indirect or punitive damages shall be specifically excluded.

2. The burden of proof shall stay with the Local Data Exporter to demonstrate that the entity outside the EEA is not liable for the violation resulting in the damages claimed by the Data Subject. The Local Data Exporter shall also have the burden to prove that it took reasonable
efforts to determine that the local data importer is able to satisfy its obligations under the BCRs. Either the Local Data Importer or the Local Data Exporter may be exempted from any liability, in whole or in part, if it is proved that they are not responsible for the event giving rise to the damage or that the Local Data Exporter took reasonable efforts to determine that the Local data importer is able to satisfy its obligations under the BCRs.

3. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the local Data Controller or, according to local labour law, a local employee) shall be taken on the initiative of the Head Controller, the Privacy Council, the Global Privacy Office, the Legal Privacy Counsel EU, the local Data Controller or the local Data Privacy Officer.

5.4 SANCTION

Would a violation of the BCRs, either by local data controller representatives or employees, be established, any appropriate disciplinary sanction or judicial action may occur, in accordance with local labour law, on the initiative of the Head Controller, the Privacy Council, the Global Privacy Office, the Legal Privacy Counsel EU, the local Data Controller or the local Data Privacy Officer, in coordination with the Office of Compliance and Ethics.

Thus, each local Data Controller and data Privacy Officer shall pay specific attention to any audit results (see paragraph 4.7) establishing non-compliance issues against representatives or employees, especially in case of:

- non compliance with the Data Protection Principles set out in paragraph 2.2 and appendix 2;
- non compliance with guidelines or procedures relating to the exercise of the rights specified in paragraph 4.1, 4.2 and 4.4 (information, access, rectification, erasure, blocking and internal complaint rights);
- non compliance with security policies designed to implement appropriate technical and organizational measures to protect personal data;
- non compliance with training programs designed to raise employee's awareness on Data Protection issues.

5.5 MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES

All BMS entities are committed to a full cooperation with the EEA data protection authorities who have competent jurisdiction. Thus:

- The relevant Data Protection Authorities shall receive, upon request, an update copy of the BCRs or all related procedures, policies or guidelines.
- The Local Data Controller shall reply within a reasonable period of time to any request addressed by a relevant Data Protection Authority with competent jurisdiction, including audit requests.
- The Local Data Controller shall apply any relevant recommendation or advice from a relevant Data Protection Authority relating to the implementation of the BCRs.
The Local Data Controller shall abide by a decision of a relevant Data Protection Authority with competent jurisdiction, related to the implementation of the BCRs, against which no further appeal is possible before competent courts.

The Legal Privacy Counsel EU or the Global Privacy Office shall be at the disposal of the relevant Data Protection Authorities for any matter related to the implementation of the BCRs.

Furthermore, members of BMS Group shall cooperate and assist each other to handle a request or complaint from an individual (see paragraph 4.4) or inquiry by Data Protection Authorities.

6. FINAL PROVISIONS

6.1 RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs

BMS undertakes that appropriate entities and employees of the BMS Group shall comply with the provisions of the BCRs, as well as with the provision of the 65/46 and 2002/50 EU Directives and applicable local laws, as provided by article 4 of the 95/46 EU Directive.

Where the local legislation requires a higher level of protection for personal data, it always will take precedence over the BCRs.

6.2 RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS

Where a local data controller requests that a non-BMS entity undertakes processing of personal data, the following safeguards shall be followed:

1. External processors located inside the EEA or in a country recognised by the EU Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the processor shall act only on instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures (see paragraph 4.5). Local Privacy Officers, in coordination with the Legal Privacy Counsel EU and the Global Privacy Office, shall be able to provide templates of the appropriate clauses to a local data controller within the Group.

2. All transfers of personal data to external controllers located out of the EEA must respect the European rules on transborder data flows (Articles 25-26 of the 95/46 EU Directive), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC.

3. All transfers of personal data to external processors located out of the EEA must respect the rules relating to the processors (Articles 16-17 of the 95/46 EU Directive) in addition to the rules on transborder data flows (Articles 25-26 of the 95/46 EU Directive), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission on February, 5, 2010 (c2010/0593).
6.3 ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

Shall a local data controller have reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the rules, he will promptly inform the Legal Privacy Counsel EU or the Global Privacy Office (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Where there shall be conflict between national law and the commitments in the BCR, the local data privacy officer and the local data controller, in coordination with the Legal Privacy Counsel EU or the Global Privacy Office, shall take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.

6.4 UPDATES OF THE BCRs

In case of, for instance, changes in laws or BMS procedures, the terms of the BCRs may be updated on the initiative of the Head Controller, in coordination with the Global Privacy Office and the legal Privacy Counsel EU.

Any substantial or non substantial update of the BCR shall be recorded and kept by the Global Privacy Office and the Legal Privacy Counsel EU. The Global Privacy Office and the Legal Privacy Counsel EU keep as well a fully updated list of the members of the Group.

BMS undertakes that appropriate information will be given, once a year, to the data subjects, the appropriate local data controllers and the competent Data Protection Authorities about any substantial update.

No transfer shall be made to a new BMS entity until this new entity is effectively bound by the BCR and can deliver compliance.

6.5 DEROGATIONS OF ARTICLE 26 EU DIRECTIVE 95/46

In accordance with article 26 of the 95/46 EU Directive and applicable local law, a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place from a Local Data Controller on condition that:
- the data subject has given his consent unambiguously to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in
general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

6.6 APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

The BCRs shall be adopted by the Head Controller, in coordination with the "Privacy Council", the Privacy Global Office and the Legal Privacy Counsel EU.

The BCRs shall take effect on the date when each BMS entity signs this BCRs agreement and, as a consequence, is legally bound. Each BMS entity recognizes to be bound by the BCRs, from the date of signature of the BCRs agreement and without any other formalities, with respect to other BMS entities already bound or about to be bound from the date of their signature, notwithstanding the date and place of signature of a BCRs agreement by each other BMS entity involved, and provided that the terms of the BCRs are strictly identical between each other. Except if a BMS entity is able to prove that the signed BCRs agreement is not strictly identical to the ones signed by other BMS entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCRs.

In the event that a Local Data Controller would be found in substantial or persistent breach of the terms of the BCRs, the Head Controller may temporarily suspend the transfer of Personal Data until the breach is repaired. Should the breach not be repaired in due times, the Head Controller shall take the initiative to terminate the BCRs Agreement. In such a case, the local Data Controller shall take every necessary step in order to respect the European rules on transborder data flows (Articles 25-26 of the 95/46 EU Directive), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

The provisions of the BCRs shall be governed by the law of the EEA Member State in which the Local Data Exporter is located.

In accordance with paragraph 5.2 and 5.3, jurisdiction shall be attributed to the courts of the Local Data Exporter.

In case of contradiction between the BCRs and the appendixes, the BCR shall always prevail. In case of contradiction between the BCRs and other global or local policies, procedures or guidelines, the BCR shall always prevail. In case of contradiction or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the 95/46 and 2002/58 EU Directives.
APPENDIX 1 : DEFINITIONS

The terms and expressions used in the BCRs are defined in this appendix, provided that these terms and expressions shall always be interpreted according to the EU 95/46 and 2002/58 Directives.

"Head Controller" shall mean BMS Headquarters located in the US, 345 Park Avenue New York City, New York 10154, which alone or jointly with others determines the purposes and means of the processing of personal data and which is in charge of the formal adoption of BCRs to be implemented within BMS Group.

"Local Data Controller" shall mean the BMS legal entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

"Local Data Exporter" shall mean the BMS legal entity located within the EEA which transfers the Personal Data outside the EEA.

"Local Data Importer" shall mean the BMS legal entity located outside the EEA which agrees to receive from the Local Data Exporter Personal Data for further Processing.

"Local Data Privacy Officer" shall mean an experienced BMS officer within a Local Data Controller who is responsible for managing business awareness and compliance with applicable data protection law and BMS privacy policies, procedures and guidelines, especially the BCRs.

"Legal Privacy Counsel EU" shall mean the senior level manager who is responsible, within the Group at European level, for managing business awareness and compliance with applicable data protection law and BMS privacy policies, procedures and guidelines, especially the BCRs.

"Global Privacy Office" shall mean the department located within the Head Controller Offices who is in charge, within the Group at worldwide level, for managing business awareness and compliance with applicable data protection law and BMS privacy policies, procedures and guidelines, especially the BCRs.
"Privacy Council" shall mean a dedicated taskforce, within BMS Group, in which all relevant professionals are represented (business units, human resources, audit and compliance, global privacy office, etc.). The Privacy Council is both in connection with the Head Controller and with a network of "Data Privacy Officers" responsible for enforcing, at local level, all defined guidelines, policies and procedures relating to Data Protection Issues.

"Office of Compliance and Ethics" shall mean the office in charge, within the Group, of an effective global compliance and ethics program. This Office benefits from a high level of independence within the firm and has overall responsibility for designing, developing and maintaining a system of procedural documents (policies, directives, SOPs and work instructions) that ensure the Company is proactively managing corporate, business unit and staff operations in accordance with applicable laws, regulations and in-house policies; routinely monitoring business unit and staff function area compliance with policies, directives and procedures; identifying potential compliance risks within the Company and facilitating a corrective action planning process to close the gaps and mitigate the risks; overseeing the prompt and thorough investigation of reported concerns about business practices or individual misconduct.


"Personal Data": shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"Processing of Personal Data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

"Recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

"Sensitive Data" shall mean Personal Data revealing directly or indirectly the racial or ethnic origin, political, philosophical or religious opinions, trade union affiliation, or related to the health or sexual life of individuals.

"Third Party" shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
"The Data Subject's Consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

"Applicable data protection law" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the EEA Member State in which the Local data exporter is established.

"Technical and organizational security measures" shall mean measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
APPENDIX 2: DATA PROTECTION PRINCIPLES

Within the scope of the BCRs, any transfer of personal data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles:

LEGAL BASIS FOR PROCESSING PERSONAL DATA

Personal data shall be processed only if:

- the data subject has unambiguously given his consent;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

LEGAL BASIS FOR PROCESSING SENSITIVE DATA

Sensitive Personal data, especially personal data concerning health, shall be processed only if:

- the data subject has given his explicit consent to the processing of those sensitive data, except where the applicable laws prohibit it;
- the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards;
- the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- the processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the consent of the data subjects;
- the processing relates to sensitive data which is manifestly made public by the data subject;
- the processing of sensitive data is necessary for the establishment, exercise or defense of legal claims;

- the processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data is processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

**PURPOSE LIMITATION**

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

In accordance with the provisions of the 95/46 EU Directive, sensitive data shall only be provided with additional safeguards.

**DATA QUALITY AND PROPORTIONALITY**

Personal data shall be processed fairly and lawfully.

Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

**AUTOMATED INDIVIDUAL DECISIONS**

Subject to local applicable law, every data subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, reliability, conduct, etc.