Bristol-Myers Squibb

Binding Corporate Rules (BCRs)

for intra-group transfers of personal data to non-EEA countries

TABLE OF CONTENTS

1 Introduction

1 Bristol Myers Squibb (BMS) agrees to follow these Binding Corporate Rules (BCRs) for its group of companies. These rules regulate how data is transferred within the BMS group from the European Economic Area (EEA) to countries outside the EEA. BMS is restating its commitment to these BCRs to ensure it continues complying with privacy laws in the European Union, including the General Data Protection Regulation (GDPR). In summary, BMS is reaffirming its commitment to data transfer rules to remain compliant with EU privacy regulations.

2 This agreement is part of Bristol-Myers Squibb's long-standing proactive approach to data privacy. BMS has an internal organization that incorporates Data Protection Principles (see Appendix B) into all decision-making, as set out in the GDPR. This organization is notable by having a global Data Risk office, Privacy Law Team, and a Data Protection Officer all working together with BMS Business Units, IT, and local teams. Local staff, working closely with our global privacy teams, enforce data protection guidelines, policies, and procedures for each country bound by this document. Our Standards of Business Conduct and Ethics also emphasize the importance of privacy and confidentiality principles.

3 As part of regular business, BMS receives, collects, maintains, and uses large amounts of personal data from individuals. This may include sensitive health information. BMS and its employees are responsible for protecting and respecting the personal information they access. BMS believes its Binding Corporate Rules are a crucial tool to effectively manage this important responsibility of protecting personal data.

4 Adopting Binding Corporate Rules is another step in BMS's full commitment to data protection compliance. More than just enabling Personal Data transfers outside the EEA, this approach broadcasts and shares our privacy culture across the BMS group. This enhances our commitment to stakeholders, partners, and others. Regarding the scope, appropriate BMS group entities and employees will follow the guidelines set out in this document and follow applicable local laws.

5 Bristol-Myers Squibb Pharmaceutical Unlimited Company (BMSI, Company Number:15797), whose offices are at Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland, a subsidiary of BMS, oversees 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. BMSI as the Head Controller, ensures continued compliance with all applicable privacy laws and has **appointed a Data Protection Officer (DPO) for Europe based in Dublin in Ireland** – the DPO works with the Privacy Law Team and Data Risk office for supervising, at a global level, the implementation of the BCRs in all appropriate BMS entities and reports directly to the highest levels of management at BMS. In addition, the DPO can inform the highest management level if any questions or problems arise during the performance of their duties. BMSI and the DPO for Europe is best placed to enforce the BCRs within the Group, coordinating efforts between the supervisory teams and the Operations team based in India and the US.

NOTE: It is important that the DPO will not have any tasks that could result in conflict of interests. The DPO is not in charge of carrying out data protection impact assessments (these are conducted by the Operations team in India and the US) is also not in charge of carrying

out audits related to the BCRs. However, the DPO will at all times be available for assisting the BCR members, and the advice of the DPO should be sought for these tasks.

6 The DPO can be contacted at any time through the eudpo@bms.com email address, by phone (+353 1 4833634) or alternatively by writing to (for the attention of the DPO) Bristol-Myers Squibb Pharmaceutical Unlimited Company (BMSI), Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland.

7 At the local level, in line with these Binding Corporate Rules (BCRs), each Local Data Controller must sign this legally binding agreement to adopt and comply with the BCRs. They are also required to take all necessary steps to ensure adherence to these provisions. Compliance will be primarily enforced through regular training programs and auditing activities. In the event of a violation of the BCRs, corrective actions—including legal or additional Technical and Organizational Security Measures—and appropriate sanctions may be imposed. These actions could target either the Local Data Controller or a local employee, depending on local labour laws. Such measures may be initiated by the Head Controller, Data Risk office, Privacy Law Team, Data Protection Officer (DPO) for Europe, the Compliance and Ethics office, or the Local Data Controller.

2 Definitions and Data Protection Principles

2.1 Definitions

The terms and expressions used in these BCRs are defined in Appendix A and should always be interpreted in accordance with the GDPR and applicable national data protection laws.

2.2 Data Protection Principles

Under these BCRs (see "Scope of the BCRs" below), any transfer of Personal Data to a third country that does not provide an adequate level of protection must comply with the data protection principles outlined below and in more detail in Appendix B These principles follow the key requirements of the GDPR:

- **Legal Basis for Processing Personal and Sensitive Data:** Personal and Sensitive Data will only be processed in accordance with the conditions set out in the GDPR.

- **Purpose Limitation:** Personal Data must be collected for specific, clear, and legitimate purposes. It should not be processed in ways that are incompatible with these purposes, unless allowed by the GDPR.

- **Data Quality and Proportionality**: Personal Data must be processed fairly and lawfully. It should be adequate, relevant, and not excessive for the purposes it was collected or processed for. The data must be accurate and, when necessary, updated. Personal Data should only be stored in a way that allows identification of individuals for as long as necessary for the purposes for which it was collected or processed.

- **Transparency**: Personal Data must always be collected and processed in a clear and transparent manner. (see section 4.1)

- **Data Subject rights**: Data Subjects have the right to exercise their legal rights regarding their Personal Data held by BMS. (see section 4.2).

- **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 (see section 4.3).

- **Security and confidentiality**: Appropriate technical and organizational security measures must be implemented to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, as well as from all other unlawful forms of processing (see section 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.

3.2 Material Scope

The nature and purposes of the Personal Data being transferred within the scope of the BCRs is detailed in Appendix C .

3.3 Corporate Scope

The Binding Corporate Rules (BCRs) will be binding on the BMS entities that are parties to the BCR Adoption Agreement outlined in Appendix E also provides a list of all BMS entities that are subject to these BCRs. Every BCR member included in Appendix E, and their associated employees, have a clear duty and legal responsibility to respect the provisions and responsibilities set out in this BCR

4 Effectiveness of the BCRs

This section outlines how BMS implements our internal policies to ensure compliance with EU data protection laws and protect personal data during international transfers within our corporate group of companies. Here are some key aspects that contribute to the effectiveness of BCRs.

4.1 Transparency and Information Rights

To make the data Processing fair, Personal Data will always be collected and further Processed on a transparent basis. Therefore:

1) The Binding Corporate Rules (BCRs) will always be easily accessible to every Data Subject. They will be uploaded on both the BMS intranet and the corporate website. Additionally, a Data Subject can request a copy of the BCRs from the Data Risk office and/or the Local Data Controller at any time.

2) All data processing activities, and any data transfers outside the EEA when applicable, must be accompanied by the relevant data protection notices.

Local Data Protection Liaisons, in coordination with the BMS Data Protection Officer (Europe) and the Privacy Law Team, will provide templates of notices to every Local Data Controller within the Group for any purpose that requires informing Data Subjects when a BMS global privacy notice is not applicable.

BMS will provide a Data Subject with at least the following information, except when they already have it:

1) the identity of the Controller(s) and any Processor(s) and of their representative(s), if any, and, when appropriate, the place in which the Local Data Importer is based outside the EEA.

2) The nature and purposes of the processing for which the data is intended, along with the legal basis for that processing. If the processing is based on consent, it should be stated that individuals have the right to withdraw their consent at any time without affecting the lawfulness of the processing that occurred before the withdrawal. If the processing is based on legitimate interests, the specific legitimate interest being pursued should also be outlined.

3) when appropriate, the purpose(s) of the transfer(s) outside the EEA and the mechanisms used to carry out such transfer(s) (including the BCRs).

Any further information such as:

1) the categories of data concerned.

2) the Recipients or categories of Recipients of the data

3) the period for which data will be retained, or if that is not possible, the criteria used to determine that period.

4) whether replies to the questions are obligatory (under contract or statute) or voluntary, as well as the possible consequences of failure to reply.

5) the existence of the right of access to, rectification of, erasure of, portability of the data concerning them as well as the right to restrict or object to the Processing of data concerning them, and the right to lodge a complaint with a Supervisory Authority.

6) If applicable, the source from which the data originated and whether it was obtained from publicly accessible sources.

7) any further information which might be necessary to ensure that the Processing is made in a transparent manner (for example, Processing through automated decision-making).

***Note**: When a new purpose or a new category of recipient arises in relation to existing data processing, the relevant information notice will be updated accordingly, and the Data Subjects will be informed.*

***Note**: If the data has not been obtained directly from the Data Subjects, BMS will provide the above information either at the time of recording the personal data or, if a disclosure to a third party is planned, no later than when the data is first disclosed.*

According to Article 14.5 of the GDPR, the information mentioned above does not need to be provided in exceptional cases where:

- the Data Subjects already have this information.
- Providing such information may be impossible or require an excessive amount of effort, especially in cases involving processing for archiving in the public interest, scientific or historical research, or statistical purposes. This is governed by the conditions and safeguards specified in Article 89(1) of the GDPR.[1] Furthermore, if the obligation to provide this information would obstruct or significantly hinder the objectives of that processing, BMS will implement appropriate measures to safeguard the Data Subject's rights, freedoms, and legitimate interests. These measures may include making the information publicly accessible.
- obtaining or disclosure is expressly laid down by Union or Member State law, which provides appropriate measures to protect the Data Subject's legitimate interests.
- Professional secrecy that is regulated by law, or situations where obtaining or disclosing information is explicitly required by law (refer to Final Provisions below).

4.2 Data Subject Rights

Data Subjects are entitled to be told what information BMS holds on them and to keep this information under control. See the following sections for more information on these rights.

4.3 Obtaining Information from BMS

Without constraint at reasonable intervals and without excessive delay or expense, confirmation of whether data related to the individual is being processed, along with the following information will be provided - including:

1) The purposes of the processing.
2) The categories of data involved.
3) The recipients or categories of recipients to whom the data is disclosed.

[1] Article 89 conditions/safeguards such as applying data minimisation principles, using pseudonymization, documenting any exclusions from certain safeguards, and paying attention to any additional EU Member State legislation related to processing data for research, scientific or public interest purposes. See the section on Article 89 for more information.

4) If possible, the anticipated duration for which the personal data will be stored, or the criteria used to determine that duration.

5) The existence of rights to rectification, erasure, restriction of processing, and objection to processing.

    i. **Rectification -** You have the right to update/correct your personal data, for example if it is inaccurate, incomplete, or not up to date. See Article 16 – Right to Rectification for more information.

    ii. **Erasure** – Please see Erasure of Personal Data.

    iii. **Restriction of Processing** – The right to request that BMS restricts, suspends, or ceases the processing of your personal data. Exceptions also apply here. If BMS lifts the restriction, we will inform you beforehand and explain our reasoning. See Article 18 in for more information.

    iv. **Objection to Processing -** You have the right to object to the use of your personal information at any time, especially if it's being used based on certain legal grounds. This includes situations where your data is being analysed to create a profile about you. If you object to the use of your data, BMS will:

        a. Stop using your information, unless

        b. BMS can prove that we have a good reason to continue processing your information.

    These reasons to continue processing must be more important than your own rights and freedoms. For example, BMS may keep processing your data if we need it for legal purposes, such as defending our company in court. See Article 21 in for more information

6) The right to lodge a complaint with a supervisory authority.

7) The existence of automated decision-making.

8) Communication to them in an intelligible form of the data undergoing Processing and of any available information as to their source.

9) The rectification, erasure, or blocking of personal data, as appropriate, if the processing does not comply with the provisions of the Binding Corporate Rules (BCRs), particularly due to the data being incomplete or inaccurate.

10) The right to object to the processing of their data at any time on compelling legitimate grounds related to their specific situation, as well as when the data is processed for direct marketing purposes.

11) To request the portability of data relating to them.

***Note**: According to the GDPR, the exercise of those rights may be subject to certain limitations.*

4.4 Erasure of Personal Data

Data Subjects will also have the right to obtain from BMS ***the erasure of their Personal Data*** without undue delay where at least one of the following applies:

1) The Personal Data are no longer necessary for the purposes for which they were collected or otherwise Processed.

2) The Data Subject withdraws their Consent on which the Processing is based, or when the storage period for which the Data Subject had Consented to has expired, and where there is no longer a legal ground for the Processing for the Personal Data

3) The Data Subject objects to the Processing of their Personal Data, including where their Personal Data is Processed for direct marketing purposes, and there are no overriding legitimate grounds for the Processing.

4) The Personal Data must be erased for compliance with a legal obligation in the Union or Member State law, including where a court or regulatory authority has ruled that the data concerned must be erased; or the Personal Data has been unlawfully Processed.

4.5 Exemptions to Erasure Requests

BMS will not need to comply with a request for erasure where Processing is necessary for:

1) Exercising the right of freedom of expression and information.

2) Compliance with a legal obligation.

3) Reasons of public interest in public health[2].

4) Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[3].

5) The establishment, exercise, or defence of legal claims.

If any of the above circumstances apply, BMS will notify the relevant BMS entity and/or third parties to whom the data has been transferred about any rectification or erasure that has

[2] In accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the GDPR. Both Article 9(2)(h) and (i) provide exceptions for processing sensitive personal data related to health and public health, ensuring such activities can be conducted legally while safeguarding individuals' rights. Article 9(3) GDPR lays down specific indications for processing carried out in the context of professional or institutional activities.

[3] In accordance with Article 89(1) of the GDPR in so far as erasing the Personal Data is likely to render impossible or seriously impair the achievement of the objectives of that Processing

been carried out, unless this is impossible or requires disproportionate effort. Additionally, BMS will inform the Data Subjects about these recipients upon request.

1) Every Data Subject will be clearly informed, in accordance with section 4.1, on how they can exercise their rights.

2) Specific guidelines and procedures will be established within the Group at the local level to ensure that the rights mentioned above are exercised effectively. All BMS employees will receive training to recognize requests related to Data Subject rights. Each request will be acknowledged and processed according to the local procedures in place.

3) A specific response will be provided to the Data Subject within one month of receiving the request.

***Note**: If the complexity or number of requests necessitates it, this one-month period may be extended by up to two additional months, in which case the Data Subject will be informed accordingly. If the request is deemed legitimate, BMS will take the necessary steps to address it promptly. If the request is denied, the reason for the denial will be communicated in writing to the Data Subject. In such cases, the Data Subject may utilize the internal complaint mechanism outlined in section 4.4.*

---

4) Local Data Protection Liaisons, in coordination with the BMS DPO (Europe), the Data Risk office, and the Privacy Law Team, will be at the disposal of both Local Data Controllers and Data Subjects to provide any help.

4.6 Automated Individual Decisions

Subject to applicable local laws, each Data Subject has **the right not to be subjected to decisions with legal consequences or significant impact**, **if those decisions are made solely based on automated data processing** aimed at evaluating personal characteristics, such as job performance, reliability, behaviour, and similar attributes.

4.7 Internal Complaint Mechanism

If a Data Subject believes that their personal data is not being processed in accordance with the Binding Corporate Rules (BCRs) or relevant local laws, they can submit a claim to BMS to request appropriate corrective actions and, if applicable, compensation (see sections 5.2 and 5.3).

1) Specific guidelines and procedures are established within the Group at the local level to ensure a consistent complaint mechanism and to provide sufficient information to Data Subjects about these procedures. **Data Subjects can submit questions or complaints through a dedicated email address (eudpo@bms.com**) or through the appropriate local contacts, for example the local HR team. The local data privacy liaison contact, in partnership with the relevant local BMS teams, will process the complaint. Regardless, all complaints by any data subject can be submitted for

processing at eudpo@bms.com, by phone (+353 1 4833634) , or to the following physical address:

Bristol Myers Squibb
Data Protection Officer
Plaza 254,
Blanchardstown Corporate Park 2,
Ballycoolin,
Dublin 15,
Ireland.
D15 T867

2) Individuals responsible for handling a claim will maintain **an appropriate level of independence in their roles**. **Complaints will be addressed without undue delay**, and in any case, within one month of submission. If the situation is complex and the complaint cannot be resolved within that timeframe, the response period may be extended by up to two additional months.

3) If the Data Subject or BMS representatives cannot resolve the claim at the local level, the complaint handling mechanism allows the Data Subject **to escalate the issue to the Data Risk office**. This office will then forward the complaint to the Compliance and Ethics office, the BMS Data Protection office (Europe), and the Privacy Law Team. The escalation process must take place within a reasonable timeframe to ensure that the complaint is addressed within the time limits specified in the previous section.

4) **Data Subjects will be informed of any remediation** measures taken by BMS entities, as appropriate. If Data Subjects are not satisfied with the decision or the measures proposed in response to their complaint, they can file a complaint with the relevant Supervisory Authorities or initiate legal action in the appropriate courts, as outlined in sections 5.2 and 5.3.

5) Each Local Data Controller and Local Data Protection Liaison will regularly report to the BMS Data Protection Officer (Europe) regarding complaints resolved at the local level. This reporting aims to identify corrective actions and improve the guidelines and procedures within the Group, especially when complaints indicate a potential "gap" in privacy compliance.

6) Complaints will be addressed fairly and, in collaboration with, the Data Subject. All BMS representatives and employees at the local level will make their best efforts to assist the Local Data Controller or the Local Data Protection Liaison in resolving a complaint.

***Note**: Nothing in the Binding Corporate Rules (BCRs) prevents individuals from filing complaints with the relevant Supervisory Authorities or initiating legal action in courts of competent jurisdiction at any time for violations of the BCRs.*

4.8 Security and Confidentiality

Each Local Data Controller must implement suitable Technical and Organizational Security Measures to safeguard Personal Data against accidental destruction, loss, alteration, unauthorized disclosure, or access. This is particularly crucial when data is transmitted over a network or subject to any other form of unlawful processing.

Considering the current state of technology and the cost of implementation, these measures should provide a level of security that is appropriate to the risks associated with the processing and the nature of the data being protected.

As a result, comprehensive information security policies and procedures will be developed and implemented within the Group. These security policies will establish necessary physical and logical measures to prevent or deter accidental destruction, modification, or unauthorized disclosure or access to Personal Data. Additionally, these policies and procedures will be regularly audited (see section 4.8).

1) Sensitive Data will be Processed with enhanced and specific security measures.

2) **Access to Personal Data is restricted to Recipients solely for the purpose of fulfilling their professional responsibilities**. Disciplinary action may be taken against any BMS employee who fails to adhere to the established information security policies and procedures.

3) Each liable BCR member must promptly notify the BMS Data Protection Officer (Europe) and the Data Risk office (DRO) of any data breaches as well as to the BCR member acting as a controller when a BCR member is acting as a processor. The DPO, in collaboration with the DRO, the Privacy Law Team and the Head Controller or the Local Data Controller who reported the breach, will document and assess the risk. The documentation will comprise of the facts relating to the personal data breach, its effects, and the remedial action taken. **BMS will notify the relevant Supervisory Authority within 72 hours** of becoming aware of the breach, unless it is determined that the breach is unlikely to pose a risk to the rights and freedoms of the affected Data Subjects.

4) If the data breach is likely to result in a high risk to these rights and freedoms, BMS will inform affected customers and employees without undue delay. Additionally, BMS will document all data breaches, including relevant details, and make this documentation available to the competent Supervisory Authority upon request (as further outlined in the Data Protection Principles in Appendix B).

4.9 Appropriate Safeguards for use of Processors

When a Local Data Controller requests that another BMS entity and/or an external party process Personal Data on its behalf, the following safeguards must be observed:

1) The Local Data Controller must select a Processor that provides adequate guarantees regarding the Technical and Organizational Security Measures for the processing to be conducted – see Article 32 Security of Processing. The chosen BMS entity must commit in writing to uphold these guarantees. Local Data Protection Liaisons, in collaboration with the BMS Data Protection Officer (Europe) and the Privacy Law

Team, can provide templates of the necessary clauses to the Local Data Controller within the Group.[4]

2) The appointed entity may only process the data according to the Controller's documented instructions, unless required to do otherwise by law.

3) The Local Data Controller must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4) takes all measures required pursuant to **Article 32**;

5) The processor shall not engage another processor without prior specific or general written authorisation of the Local Data Controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

6) Where a processor engages another processor for carrying out specific processing activities on behalf of the Local Data Controller, the same data protection obligations as set out in the contract or other legal act between the Controller and the Processor be imposed on that other processor by way of a contract or other legal act.

7) A processor should make every effort to assist the controller in ensuring compliance with the obligations pursuant to **Articles 32** to **36** taking into account the nature of processing and the information available to the processor.

8) Upon completion of the work, the appointed entity must either delete all transferred data or retain it if there are legal obligations to do so. In such cases, appropriate Technical and Organizational Security Measures must be implemented to protect Personal Data from accidental or unlawful processing.

4.10 Accountability

BMS entities that are bound by the Binding Corporate Rules (BCRs) are responsible for demonstrating compliance with Data Protection Principles. Thus:

1) Each entity must maintain a written record (including electronic formats) of all processing activities. A copy of this record will be provided to the competent Supervisory Authorities upon request.

2) Data Protection Impact Assessments (DPIAs) must be conducted for processing activities that pose high risks to the rights and freedoms of Data Subjects.

3) When processing is based on consent, each entity relying on that consent must be able to demonstrate that the Data Subject has given their consent for the processing of their Personal Data.

[4] That meet the requirements of Article 28(3) of the GDPR. Article 28(3) of the GDPR outlines specific requirements that must be included in the contract between a data controller and a data processor. See Article 28 (3) for more information.

4) All BMS entities bound by the Binding Corporate Rules (BCRs) will maintain appropriate policies to ensure compliance with the BCRs and to incorporate the principles of privacy by design and by default.

4.11 Training Programs

Appropriate and up-to date training on these Binding Corporate Rules are provided to BMS workers that have permanent or regular access to personal data and who are involved in the collection of data or in the development of tools used to process personal data. Privacy training is an integral part of professional development within the Group:

1) The BCRs, along with all related guidelines, procedures, and policies, are uploaded to the BMS corporate intranet, ensuring permanent access for all employees.

2) Every new BMS employee are granted access to the BCRs and related materials. Internal communications will also be distributed within the Group to raise awareness about the BCRs.

3) New employees are required to complete a privacy compliance training program. Additionally, all employees must participate in this program on a yearly basis. Upon completion of the training, employees must pass a knowledge check (certification) to confirm their understanding of privacy issues.

4) Employees who collect, process, or have access to Personal Data may receive additional specialized training programs (for example, training related to HR Personal Data, health data, and so on.). The BMS DPO (Europe) and the Privacy Law Team provide quarterly ad hoc training calls through a range of channels (including business unit team calls, market lawyer privacy sessions, and so on) that will cover in part the importance of the BCRs in relation to internal transfers of data and any updates to the legislation that might affect BMS compliance with the BCRs.

5) At the local level, each Controller and/or Data Privacy Officer/Privacy Law Team is encouraged to enhance the privacy training programs by incorporating relevant training materials. Local Data Importers are also trained on the management of requests from public authorities made to them, including the procedure for notifying the BMS DPO, Data Risk Office and Privacy Law Team as soon as any such request is received. Responding to such requests is detailed in the BMS Government Data Request Procedure.

6) Privacy training programs will be reviewed and approved by the Local Data Privacy Liaisons, the Data Risk office, the BMS DPO (Europe), and the Privacy Law Team. Procedures related to privacy training programs will undergo regular audits (see the section Audit Program below).

4.12 Audit Program

Data protection audits will be conducted regularly (at least once every three years) by internal accredited audit teams to ensure that the Binding Corporate Rules (BCRs) and related policies, procedures, and guidelines are current and effectively implemented across the entities signed up to this agreement - if there are indications of non-compliance these will subsequently assessed and addressed to ensure verification of compliance with the BCRs. The BMS Audit Team will not monitor all aspects of the BCRs each time a BCR

member is audited, however within the three-year cycle mentioned above, all aspects of the BCR-C will be monitored at appropriate regular intervals for that BCR member.

1. Data protection audits will encompass all aspects of the BCRs and related policies, procedures, and guidelines, including methods for implementing corrective measures. For example, the audit will cover, applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCRs, review of the contractual terms used for the transfers out of the Group to controllers or processors of data, corrective actions, etc.), including methods and action plans ensuring that corrective actions have been implemented. However, the scope of each audit may be narrowed to focus on specific aspects of the BCRs and/or related materials. The frequency will be determined on the basis of the risk(s) posed by the processing activities covered by the BCRs to the rights and freedoms of data subjects, but not less that every 3 years.

2. BMS Global Internal Audit will oversee the BCR audit program, andwill directly decides on the data protection audits frequency in consultation with the Head Controller, the Compliance and Ethics office, the Local Data Controller, the Local Data Privacy Liaison, the BMS Data Protection Officer (Europe), or the Privacy Law Team. Those conducting the audits (BMS GIA) will maintain an appropriate level of independence in their duties. Specific audits (ad hoc audits) may also be requested by the Privacy officer or other related Function at anytime.

3. The results of all audits will be communicated to BMSI Officers, the BMS Data Protection Officer (Europe), the Data Risk office, and/or the Local Data Protection Officer, the Privacy Law Team, the BMS Board of Directors and the board of the liable BCR member, and/or the Local Controller.

4. A competent Supervisory Authorities may request a copy of these audit results. Each Local Data Controller agrees to be audited by a competent Supervisory Authority and to comply with their guidance regarding any issues related to the BCRs.

5. As outlined in section 5.1.3 below, Local Data Privacy Liaisons will report annually to the Head Controller and the BMS Data Protection Officer (Europe) on all actions and measures taken concerning data protection issues (such as training programs, inventory of Personal Data Processing activities, complaint management, etc.). Each Local Data Privacy Liaison will also take necessary steps to ensure that Local Data Controllers comply with the BCRs. To facilitate this, a "BCR compliance checklist" will be used at the local level for compliance checks.

6. The BMS Data Protection Officer (Europe) will also provide regular reports to the Head Controller regarding BCR implementation within each Local Data Controller.

7. Based on audit results and the reports mentioned above, the Head Controller, BMS Data Protection Officer (Europe), the Data Risk office and/or Privacy Law Team will determine any necessary legal measures or Technical and Organizational Security Measures to enhance data protection management within the Group at both global and local levels.

5 Binding Nature of the BCRs

5.1 Compliance and Supervision

BMS fully integrates Data Protection Principles into its decision-making process. This process is overseen by two global teams: the Data Risk office and the Privacy Law Team, and by the BMS Data Protection Officer (Europe**)**. These teams work closely with the Head Controller and a network of local Data Protection Liaisons who are responsible for enforcing all established guidelines, policies, and procedures related to data protection at the local level.

Compliance with these guidelines and procedures is supported by training programs and regular auditing activities for all employees. The importance of privacy and confidentiality is emphasized in our Standards of Business Conduct and Ethics.

The Head Controller has designated the BMS Data Protection Officer (Europe) and the Privacy Law Team to oversee the global implementation of the Binding Corporate Rules (BCRs) across all relevant BMS entities.

At local level, each local Data Protection Liaison will be responsible for the implementation of the BCRs under the supervision of the BMS Data Protection Officer and the Privacy Law Team. Therefore:

1) Each Data Protection Liaison must take all necessary steps to ensure that Local Data Controllers comply with the provisions of the Binding Corporate Rules (BCRs). To facilitate this, a “BCR compliance checklist” will be used at the local level for compliance assessments. Data protection audits conducted by the Global Internal Audit team, the BMS Data Protection Officer (Europe), or the Privacy Law Team may focus on how these compliance checks are implemented locally.

2) Local Data Protection Liaison, in collaboration with the BMS Data Protection Officer (Europe) and the Privacy Law Team, will always be available to assist both Local Data Controllers and Data Subjects with any data protection issues, particularly those related to the BCRs.

3) Each year, local Data Protection Liaisons, in coordination with the BMS Data Protection Officer (Europe) and the Privacy Law Team, will report to the Head Controller on all actions and measures taken concerning data protection issues (such as training programs, inventory of Personal Data Processing activities, complaint management, etc.), with a specific focus on the implementation of the BCRs.

4) Local Data Controllers and Local Data Protection Liaisons will regularly report to the BMS Data Protection Officer (Europe) and the Privacy Law Team regarding complaints resolved at the local level. This reporting aims to identify corrective actions and improve guidelines and procedures within the Group, especially where complaints may indicate a "gap" in privacy compliance.

5) Local Data Protection Officers, in coordination with the office of the BMS DPO (EUROPE) and the Privacy Law Team, will provide appropriate templates (e.g., information notices, clauses, etc.) to each Local Data Controller within the Group for any data protection-related purposes.

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

1) The BMS Data Protection Officer (Europe) and the Privacy Law Team will regularly report to the Head Controller and the about the implementation of the BCRs within each Local Data Controller.

2) Data protection audits shall be decided directly by the Global Internal Audit team or upon specific request of a Local Data Privacy Liaison, the Compliance and Ethics office, the BMS Data Protection Officer (Europe) or the Privacy Law Team. The results of all audits or reports shall be communicated to the Data Protection office, the office of the BMS DPO (EUROPE) and the Privacy Law Team.

3) Thanks to the audit results and the reports mentioned above, the Head Controller, the Compliance and Ethics office, the Data Risk office, the Privacy Law Team, the BMS Data Protection Officer (Europe), a Local Data Controller or a Local Data Privacy Liaison shall decide any appropriate 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 corrective measure (legal measures or Technical and Organizational Security Measures) 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 Data Risk office, the Privacy Law Team, office of the BMS DPO (EUROPE), a Local Data Controller or a Local Data Protection Officer, in coordination with the Compliance and Ethics office.

5) Privacy training programs shall be reviewed and approved by BMS senior Officers, in coordination with the Privacy Law Team, the BMS Data Protection Officer (Europe) and Local Data Privacy Liaisons. Procedures related to privacy training programs shall be regularly audited (see section 4.8).

6) All Local Data Exporters agree to monitor, on an ongoing basis, and where appropriate in collaboration with Local Data Importers, developments in the third countries to which the Local Data Exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

A Data Subject will have the right to enforce, as a third party beneficiary, the provisions of these BCRs – particularly the Data Subject Rights outlined in section 4.2 Data Subject Rights.. Therefore:

1) Each Data Subject has the right to bring their case to the appropriate Supervisory Authority at their convenience. This authority may be in the Data Subject's country of habitual residence, their workplace, or where the alleged infringement occurred. Additionally, the Data Subject can take their case to a competent court in the EU (to seek judicial redress), either in the country where BMS has an establishment or in their own EU country of habitual residence, for any breach of the Binding Corporate Rules (BCRs)

2) According to the relevant provisions in section 5.3, each Data Subject who has suffered material or non-material damage will be entitled to receive compensation (e.g. judicial remedies).

3) The BCRs will always be readily available to every Data Subject. Furthermore, a Data Subject will always be able to obtain, upon request, a copy of the BCRs from the Local Data Protection Officer, the Local Data Controller, the BMS DPO (Europe), and/or the Privacy Law Team.

5.2 Liability

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

1) Each Local Data Exporter agrees to monitor the compliance of the relevant Local Data Importer with these Binding Corporate Rules (BCRs). The Local Data Exporter accepts responsibility for any violations of these BCRs by the Local Data Importers and commits to taking necessary actions to address such violations. They also agree to pay any compensation for material and non-material damages awarded to Data Subjects by the courts mentioned in section 5.2, unless the Local Data Importer has already paid the compensation or complied with the court order. The Local Data Exporter must have sufficient financial resources available to cover any compensation payments for breaches of the BCRs. Unless prohibited by applicable European Union or Member State law, liability between the Local Data Importer and Local Data Exporter will be limited to actual material and non-material damages, specifically excluding indirect or punitive damages.

2) Each Local Data Exporter is responsible for proving that the entity outside the EEA, which received Personal Data from them, is not liable for any violations that resulted in damages (material and non-material) claimed by the Data Subject. The Local Data Exporter may be fully or partially exempt from liability if it can be demonstrated that the entity outside the EEA is not responsible for the incident that caused the damage.

3) If a violation of the BCRs is confirmed, corrective actions (including legal measures or Technical and Organizational Security Measures) and any appropriate sanctions (against the Local Data Controller or, in accordance with local labour law, a local employee) will be initiated by the Head Controller, the Data Risk office, the Privacy Law Team, the BMS Data Protection Officer (Europe) the Local Data Controller, or the Local Data Protection Liaison.

4) All BCR members to this agreement also accept that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80 of the GDPR.

5.3 Sanction

If a violation of the BCRs is confirmed, whether by representatives or employees of the Local Data Controller, appropriate disciplinary actions or legal measures may be taken in accordance with local labour laws. This process will be initiated by the Head Controller, the Data Risk office, the Privacy Law Team, the BMS Data Protection Officer (Europe), the

Local Data Controller, or the Local Data Protection Liaison, in coordination with the Compliance and Ethics office.

Therefore, each Local Data Controller and Data Privacy Liaison must pay close attention to any audit results (see section 4.9) that identify non-compliance issues involving representatives or employees, particularly in cases of non-compliance with the following:

a) Data Protection Principles set out in **Appendix B**.

b) Guidelines or procedures relating to the exercise of the data subject's rights.

c) Security policies designed to implement appropriate Technical and Organizational Security Measures to protect Personal Data.

d) Training programs designed to raise employee's awareness on data protection issues.

5.4 Mutual Assistance and Cooperation with Supervisory Authorities

All BMS entities are committed to a full cooperation with the competent EEA Supervisory Authorities. Therefore:

1. The competent Supervisory Authorities will receive, upon request, an updated copy of the BCRs or all related procedures, records of processing activities, policies, guidelines, or training materials specified in section 4.7.

2. The Local Data Controller will reply within a reasonable period to any request addressed by a competent Supervisory Authority, including audit requests. Every BMS entity party to this agreement agrees to:

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

    - to take into account their advice, and

    - to abide by decisions of these SAs on any issue related to these Binding Corporate Rules.

3. The Local Data Controller will apply any relevant recommendation, advice and decisions from a competent Supervisory Authority relating to the implementation of the

4. The Local Data Controller will comply with the decision of a competent Supervisory Authority regarding the implementation of the BCRs. Any dispute related to the Competent SAs' exercise of supervision of compliance with these BCRs will be resolved by the courts of the Member State of that SA, in accordance with that Member State's procedural law. The BCR members agree to submit themselves to the jurisdiction of these courts.

5. The BMS Data Protection Officer (Europe) or the Privacy Law Team are always at the disposal of the competent Supervisory Authorities for any matter related to the implementation of the BCRs.

Furthermore, members of the Group will cooperate and assist each other to handle a request or complaint from an individual or inquiry by Supervisory Authorities.

6 Final Provisions

6.1 Actions when National Legislation Impacts BCR Commitments

1 BMS commits to ensuring that the appropriate entities and employees within the Group comply with the provisions of the Binding Corporate Rules (BCRs) and relevant local laws.

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

3 BMS commits to ensuring that it has no reason to believe that the laws and practices governing the processing of Personal Data by Local Data Importers in third countries—such as requirements for disclosing Personal Data or authorizations for public authority access—will prevent these Local Data Importers from fulfilling their obligations under the BCRs. This is based on the understanding the laws assessed on the third country respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with this agreement. Before any transfers of Personal Data (including data in transit), BMS will conduct an assessment that considers:

a) the specific circumstances of the transfers, including the location of the processing, including storage,

b) the purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials), categories and format of the personal data transferred;

c) the types of entities involved in the processing (the data importer and any further recipient of any onward transfer) and transmission channels used.

d) the laws and practices of the destination countries, considering relevant limitations and safeguards, and

e) the contractual, technical, and organizational security measures established under these BCRs, including those applied during transmission and processing in the destination country.

4 BCR members must document appropriately such a transfer assessment, as well as the supplementary measures selected and implemented. The documentation will be made available to the competent SAs upon request.

5 When a Local Data Importer can no comply with these BCRs, *for whatever reason*, **the Local Data Importer (liable BCR member) will promptly notify the Local Data Exporter and where possible the data subject** when the BCR liable member**:**

- receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of personal data transferred according to these Binding Corporate Rules - the notification will include

information about the personal data requested, the requesting authority, the legal basis for the request and the response provided.

- The Local Data Importer becomes aware of any direct access by public authorities to personal data transferred governed by these Binding Corporate Rules in accordance with the laws of the country of destination; the notification will include all information available to the Local Data Importer.

NOTE: BMS will promptly identify **appropriate supplementary measures** to be adopted by the Local Data Exporter and/or Local Data Importer to address the situation. This information will also be provided to the liable BCR member(s).

These **appropriate supplementary measures** will be identified through an assessment, involving the Liable BCR members and the Data Protection Officer (and relevant Privacy functions). All Liable BCR members will be informed about the results of this assessment and the supplementary measures that have been identified for implementation.

6 In the event of a conflict between national law and the commitments outlined in the BCRs, the Local Data Privacy Liaison and the Local Data Controller, in coordination with the BMS Data Protection Officer (Europe) or the Privacy Law Team and the liable BCR member will determine the appropriate course of action and consult the competent Supervisory Authority if there is any uncertainty. In any event, if the Local Data Exporter is in breach of these BCR commitments, or unable to comply with them, the **Local Data Exporter will suspend the transfer i**f BMS determines that adequate safeguards cannot be ensured or if instructed to do so by the competent Supervisory Authority, until compliance is again ensured, or the transfer is ended. Following such a suspension, the Local Data Exporter may choose to terminate the transfer (or series of transfers) if compliance with the BCRs is not restored within one month of suspension, and request that any Personal Data transferred before the suspension be returned to them or that it be destroyed or deleted by the Local Data Importer. If the Local Data Exporter and Local Data Importer agree that the data may be kept by the Local Data Importer, protection must be maintained in accordance with Chapter V of the GDPR.[5]

7 BMS also commits, that the liable BCR member(s) and the Data Protection Officer will be involved and informed in such assessment inform all other BCR members of the assessment carried out and of its results, so that the identified supplementary measures can be applied in case the same type of transfers is carried out by any other BCR member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

8 If any BMS entity subject to the BCRs believes that a provision of applicable local law in a non-EEA country could significantly undermine the guarantees provided by the BCRs, it will promptly notify the Local Data Exporter, the BMS Data Protection Officer and the Privacy Law Team.

[5] Chapter V of the General Data Protection Regulation (GDPR) deals with the transfer of personal data to third countries or international organizations. The main goal is to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data is transferred outside the European Union.

9 The Local Data Importer will, at the choice of the Local Data Exporter, immediately return or delete the personal data that has been transferred under the BCRs in its entirety, where:

• the Local Data Exporter has suspended the transfer, and compliance with this BCR is not restored within a reasonable time, and in any event within one month of suspension; or

• the Local Data Importer is in substantial or persistent breach of the BCRs; or

• the Local Data Importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR-C.

---

*NOTE: The same commitments should apply to **any copies of the data**. The Local Data Importer **will certify the deletion of the data** to the Local Data Exporter.*

Until the data is deleted or returned, the Local Data Importer will continue to ensure compliance with these Binding Corporate Rules.

BMSI will then report the issue to the competent Supervisory Authority, unless prohibited by law enforcement authorities (such as restrictions under criminal law aimed at preserving the confidentiality of an investigation). This includes any legally binding requests for disclosure of Personal Data from law enforcement or state security bodies, as well as any direct access these authorities may have to Personal Data transferred under the BCRs.

10 In such cases, the competent Supervisory Authority will receive information about the data requested, the requesting body, and the legal basis for the disclosure (unless prohibited by applicable law). If suspension and/or notification of such requests are not allowed, BMSI will make documented efforts to obtain permission to waive that prohibition to share as much information as possible as soon as possible. The Local Data Importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by these BCRs and will make it available to the competent Supervisory Authority upon request.

11 BMS will assess the legitimacy of requests for disclosure, particularly determining whether they fall within the authority granted to the requesting public body. If, after careful evaluation, BMS concludes that there are reasonable grounds to believe the request is unlawful under local laws, international law obligations, and/or principles of international comity, it will challenge the request. Additionally, BMS will explore avenues for appeal under similar conditions.

12 When contesting a disclosure request, BMS will seek interim measures aimed at suspending the effects of the request until a judicial decision is rendered. BMS will document its legal assessment, and any challenges related to the disclosure request. To the extent permitted by destination country laws, BMS will make this documentation accessible to the competent Supervisory Authority upon request. If the data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information on the disclosure request, it will, without undue delay, inform the data exporter accordingly.

13 BMS will refrain from disclosing Personal Data unless compelled to do so by procedural requirements. When responding, BMS will provide minimal information permissible under a reasonable interpretation of the request.

14 The Local Data Controller commits to taking into account any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the Binding Corporate Rules, including measures applied during the transmission and to the processing of the personal data in the country of destination. Some examples are listed below.

Logging	BMS maintains access logs, to ensure recording of access to systems and processes handling personal data.
Access Controls	BMS ensures that appropriate access and revocation controls with periodic managerial reviews when necessary, depending on the nature of processing activities
Confidentiality, Integrity, and Availability	BMS implements, when necessary appropriate NIST Framework controls to ensure confidentiality, integrity, and availability of personal data
Accountability	BMS, in addition to adhering to the NIST Audit & Accountability Controls, demonstrates accountability through a comprehensive Security Training and Awareness Program. This program includes mandatory cybersecurity awareness training for all employees and contractors. Additionally, several other training courses are offered, covering topics such as phishing fundamentals, remote working safety, manufacturing security, and data protection. The Chief Information Security Officer and the Enterprise Learning Services Team (ELS) are responsible for overseeing the training program. They ensure that training is conducted effectively and that compliance with completion requirements is tracked, monitored, and escalated as necessary.
Monitoring	BMS ensures monitoring, security assessment and authorization controls by adopting NIST standards when necessary. BMS also engages in active monitoring to ensure Availability. Security Monitoring, System configuration. Security Review - performed at a minimum annually Data Loss Prevention & Monitoring - Designed to detect and prevent potential data breaches, exfiltration transmissions. Appropriate controls are also in place to monitor, detect and/or blocks sensitive data while in use, in motion and at-rest.
System Configuration	BMS adopts appropriate NIST Controls for systems configuration when necessary
Back-Up & Disaster Recovery	BMS ensures appropriate back up controls based on NIST Contingency Planning Controls

Pseudonymization & Encryption	BMS has adopted appropriate identification and Authentication Controls based on NIST framework controls. Application of such controls are dependent on nature of processing activities
Sub-Processor Controls	BMS maintains an enterprise wide Third Party Risk Management (TPRM) standard. Additionally, BMS has a transition document outlining the rollout of its overall TPRM program and the various categories of suppliers and services being utilized. Both documents are reviewed annually by senior management. Under the TPRM framework, critical and major risk third parties are evaluated using an inherent risk questionnaire that generates an inherent risk rating across different security domains. This rating determines the level of assessment required for each supplier. BMS conducts pre-contract due diligence based on individual risk categories, and for certain third parties, background checks are performed by the ethics team. Standard contract templates include requirements related to these areas. Furthermore, BMS conducts periodic assessments of both cybersecurity and physical security. The TPRM framework includes a comprehensive termination and offboarding process, which features a termination checklist that ensures the return of BMS data, revocation of access, and termination of access to systems or facilities. The IT team then confirms that access has been revoked for all users.
Protection in Transit Protection at rest	Commercially available encryption software is used for data in transit and at rest.
Certification	BMS endeavors to create device certifications to limit access to certified users.
Physical Security	BMS maintains physical security standards that addresses the following: Facility access and related electronic access: - Facility intrusion monitoring, detection, and response - CCTV surveillance for sensitive areas - Employee anti-tailgating; and Visitor access controls and logging - Log retention timelines. - Access restrictions for terminated employees
IT security governance and management	BMS maintains a detailed organizational chart as well as defined responsibilities across the Information Security 'Towers'. Each tower has defined roles and responsibilities. Structure IT policies have been created in the following areas: - Access & Password Management; - Business Continuity, - Application Security; - Network Security; - Physical & Environmental Security; - Disaster Recovery; - Asset Management; - Data Classification;

	- Incident Management; - Third Party Security Management; - Change Management; - Data Encryption; - Configuration Management;

15 The Local Data Controller will take into account the laws and practices of the third country of destination relevant in light of the circumstances of the transfer , including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards.

Note: If a Local Data Importer is prevented from notifying the Local Data Exporter and /or the data subject, the Local Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the data exporter

---

6.2 Restrictions on Transfers and Onward Transfers

Where a Local Data Controller requests that a non-BMS entity undertakes Processing of Personal Data, the following safeguards will be followed:

1) External Processors located within the EEA or in a country recognized by the EU Commission as providing an adequate level of protection must be bound by a written agreement. This agreement will specify that the Processor can only act on instructions from the Controller and is responsible for implementing adequate security and confidentiality measures. Local Data Protection Liaisons, in coordination with the BMS Data Protection Officer (Europe) and the Privacy Law Team, will provide suitable templates for these clauses to Local Data Controllers 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, for instance by making use of the relevant module(s) of the EU Standard Contractual Clauses or any clauses replacing, amending, or editing them which are approved by the EU Commission.

3) All transfers of Personal Data to external Processors located out of the EEA must respect the rules relating to Processors (see Articles 28-29 of the GDPR) in addition to the rules on transborder data flows, for instance by making use of the relevant module(s) of the EU Standard Contractual Clauses approved under EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

6.3 Updating the BCRs

1 In the event of changes to laws or BMS procedures (for example, new guidance issued by the European Data Protection Board), the terms of the BCRs may be updated by the Head Controller, in coordination with the Privacy Law Team and the BMS Data Protection Officer (Europe).

2 Any substantial or minor update to the BCRs will be documented and maintained by both the Privacy Law Team and the BMS Data Protection Officer (Europe), including keeping a fully updated list of Group members.

3 BMS commits to providing appropriate information without undue delay on an annual basis to all entities bound by these BCRs, data subjects, relevant Local Data Controllers, and competent Supervisory Authorities regarding any updates with brief explanations of the changes made. Any significant modifications to the BCRs that could affect their validity or the level of protection they offer will be promptly communicated to the competent Supervisory Authority.

4 The relevant Supervisory Authority will also be notified once a year in instances where no changes have been made.

5 The annual update or notification will also include the renewal of the confirmation related to the Liable BCR member(s) having sufficient assets, or has made appropriate arrangements, to enable itself to pay compensation for damages resulting from a breach of these BCRs.

6 No transfer will be initiated to a new BMS entity until that entity is effectively bound by the BCRs and demonstrates compliance capabilities.

6.4 GDPR Article 49 Derogations

Nothing in these BCRs should be interpreted as limiting BMS's ability to use alternative data transfer mechanisms permitted under the GDPR, where applicable.

According to Article 49[6] of the GDPR and relevant local laws, a transfer, or series of transfers of Personal Data to a third country that does not provide an adequate level of protection may occur from a Local Data Controller, provided that certain conditions are met:

- **Consent** - The data subject has explicitly consented to the proposed transfer after being informed of the possible risks involved due to the absence of an adequacy decision and appropriate safeguards.

- **Contractual Necessity** - The transfer is necessary for performing a contract between the data subject and the controller or for implementing pre-contractual measures requested by the data subject.

- **Vital Interests Protection** - The transfer is made necessary to protect vital interests of either the data subject or other persons who cannot consent physically or legally.

- **Public Registers Consultation** – Transfers from public registers intended to inform the public or those demonstrating legitimate interest, provided conditions under domestic law are met.

6.5 Applicable Law

The BCRs will be adopted by the Head Controller in coordination with the Data Risk office, the Privacy Law Team, and the BMS Data Protection Officer (Europe). The provisions of

[6] Article 49 of the GDPR outlines specific conditions under which personal data can be transferred to third countries or international organizations in the absence of an adequacy decision or appropriate safeguards.

the BCRs will be governed by the law of the EEA Member State where the Local Data Exporter is located.

6.6 Termination

If a Local Data Controller is found to be in substantial or persistent breach of the BCRs, the Head Controller may temporarily suspend the transfer of Personal Data until the breach is resolved. If the breach is not resolved in a timely manner, the Head Controller will terminate the BCRs for that specific Local Data Controller. In such cases, the Local Data Controller must take all necessary steps to comply with European regulations on transborder data flows such as utilizing the EU Standard Contractual Clauses approved by the EU Commission.

Any BCR member acting as data importer, which ceases to be bound by these BCRs, may keep, return, or delete the personal data received under these BCRs.

6.7 Jurisdiction

Jurisdiction will be attributed in accordance with sections 5.2 and 5.3.

6.8 Interpretation of Terms

In the event of a conflict between the BCRs and the Appendices, the BCRs will take precedence. Similarly, if there is a contradiction between the BCRs and any other global or local policies, procedures, or guidelines, the BCRs will prevail. Furthermore, in cases of contradiction or inconsistency, the terms of the BCRs will be interpreted and governed in accordance with the provisions of the GDPR.

Appendix A Definition of Terms and Relevant GDPR Articles

A.1 Definitions

The terms and expressions used in the BCRs are defined in this section, provided that these terms and expressions will always be interpreted according to the GDPR.

"**Applicable Data Protection Law**" means the legislation protecting the fundamental rights and freedoms of individuals and their right to privacy with respect to the Processing of Personal Data applicable to a Controller in the EEA Member State in which the Local Data Exporter is established.

"Supervisory Authority (SA)" - An independent public authority established in each EEA/EU Member State to oversee and enforce compliance with data protection laws.

"Competent SA(s)"- the EEA/EU Data Protection Supervisory Authority competent for the Local Data Exporter for a specific transfer.

"**Consent**" is defined as a freely given, specific, informed, and unambiguous indication of the data subject's wishes, signifying agreement to the processing of their personal data through a clear affirmative action.

"**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

- "**Data Risk office**" refers to the internal privacy operations team responsible for tasks such as:
    - Breach notification reporting
    - Handling data subject requests
    - Maintaining records of processing activities
    - Providing training and awareness initiatives

BMS Data Protection Officer (Europe) - the registered Data Protection Officer in Europe for BMS, responsible for monitoring compliance with the GDPR, and other EU and Member State provisions relating to data protection, and the BCRs.

GDPR (General Data Protection Regulation) - the European Union Regulation number 2016/679 entitled 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC'.

Privacy Law Team - the department located within the Head Controller 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.

BMS Group - BMS and its affiliates.

Head Controllers – Bristol-Myers Squibb Pharmaceutical Unlimited Company (BMSI), whose offices are at Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland, a subsidiary of Bristol Myers Squibb Company (located in the US, Route 206 & Province Line Road, Princeton, New Jersey 08543 United States), 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.

Local Data Controller - the BMS legal entity that, either independently or in collaboration with others, determines the purposes and means of processing Personal Data within a specific local context. When national or Community laws or regulations specify the purposes and methods of processing, the Controller or the criteria for their designation may be defined by those laws.

Local Data Exporter - BMS legal entity located within the EEA which transfers the Personal Data outside the EEA.

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

Local Data Protection Liaison - an experienced BMS employee, based within a Local Data Controller, who is responsible for managing business awareness and compliance with Data Protection Law and BMS privacy policies, procedures, and guidelines, especially the BCRs.

Compliance and Ethics office - The Compliance and Ethics office at Bristol Myers Squibb (BMS) is responsible for promoting and ensuring adherence to legal and regulatory requirements, as well as the company's internal policies and ethical standards. This office develops and implements compliance programs, conducts training and education, monitors, and audits business practice, investigates potential violations, and provides guidance to employees to foster a culture of integrity and ethical behaviour throughout the organization.

Data Subject - Under EU data protection law, this term refers to a natural person who can be identified, directly or indirectly, by reference to identifiers such as a name, identification number, location data, or other specific factors related to their identity. This definition encompasses any individual whose personal data is processed by an BMS.

Personal Data - any information that relates to an identified or identifiable natural person ("Data Subject").

Processing - any operation or series of operations performed on Personal Data, regardless of whether they are carried out by automated means. This includes activities such as:

- Collection
- Recording
- Organization
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure through transmission or dissemination
- Making data available in other ways
- Alignment or combination
- Blocking
- Erasure
- Destruction.

Processor - a natural or legal person, public authority, agency, or any other entity that processes Personal Data on behalf of the Controller.

Recipient - natural or legal person, public authority, agency, or any other entity to whom data is disclosed, regardless of whether they are a third party. However, authorities that

receive data as part of a specific inquiry in accordance with the law are not considered recipients.

Sensitive Data - Personal Data that reveals, directly or indirectly, a person's racial or ethnic origin, political opinions, philosophical or religious beliefs, or trade union membership. It also includes genetic data or biometric data processed for the purpose of uniquely identifying an individual, as well as Personal Data related to a person's health, sex life, or sexual orientation.

Supervisory Authority - an independent public authority which is established by a Member State.

Technical and Organizational Security Measures - designed to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. This includes safeguards specifically aimed at securing data during transmission over a network, as well as protection against all other unlawful forms of processing.

A.2 Related Regulation (EU) 2016/679 (GDPR) Articles Referenced in this Document

This section contains GPDR Articles that are referenced in this document, using the official text where appropriate.

A.2.a Article 6.1 – Lawful Grounds for Processing

Official text:

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. 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;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. 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;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

A.2.b Article 16 – Right to Rectification

Official text:

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

A.2.c Article 80

Official text:

Article 80(1) of Regulation (EU) 2016/679 (GDPR) grants data subjects the right to mandate non-profit bodies, organizations, and associations to lodge data privacy complaints with supervisory authorities and seek judicial remedies. See here for more information on this particular article. Official text:

1) The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in **Articles 77**, **78** and **79** on his or her behalf, and to exercise the right to receive compensation referred to in **Article 82** on his or her behalf where provided for by Member State law.

2) Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

A.2.d Article 10

Official text:

Article 10 of the General Data Protection Regulation (GDPR) is a complementary provision to the Law Enforcement Directive (LED). It ensures that criminal data processing is carried out in accordance with GDPR principles and appropriate safeguards when the LED is not directly applicable. Article 10 only applies to the personal data of offenders or suspected offenders. Official text:

1. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

A.2.e Article 18

Official text:

Article 18 of the GDPR grants individuals the right to obtain restriction of processing of their personal data by a data controller. This means that while the data can be stored, most other processing actions (such as deletion) will require the individual's permission. One specific scenario for this right is when the accuracy of personal data is contested by the data subject, allowing the controller time to verify its accuracy. Official text:

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

1) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

2) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

3) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

4) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

A.2.f Article 21

Official text:

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of **Article 6(**1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding **Directive 2002/58/EC**, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to **Article 89(**1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

A.2.g Article 22 Automated individual decision-making, including profiling

Official text:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

    a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

    b. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

    c. is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

A.2.h Article 23 (1)

Official text:

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its

provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a. national security;

b. defence;

c. public security;

d. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

f. the protection of judicial independence and judicial proceedings;

g. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i. the protection of the data subject or the rights and freedoms of others;

j. the enforcement of civil law claims.

A.2.i Article 28 (3)

Official text:

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest
b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. takes all measures required pursuant to **Article 32**;

d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor.
e. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in **Chapter III;**
f. assists the controller in ensuring compliance with the obligations pursuant to **Articles 32** to **36** taking into account the nature of processing and the information available to the processor;
g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

A.2.j Article 29

Official text:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

A.2.k Article 32

Official text:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a. the pseudonymisation and encryption of personal data;

   b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in **Article 40** or an approved certification mechanism as referred to in **Article 42** may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

A.2.l Article 36

Official text:

Article 36 of the GDPR is about prior consultation. It requires the Local Data Controller to consult the supervisory authority before processing personal data that would result in a high risk to the rights and freedoms of the data subjects, as identified by a data protection impact assessment. The supervisory authority has to provide written advice to the controller within eight weeks, or longer if the processing is complex, if it finds that the processing would infringe the GDPR.

Official text:

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. [2]That period may be extended by six weeks, taking into account the complexity of the intended processing. [3]The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. [4]Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

    1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

    2. the purposes and means of the intended processing;

    3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

    4. where applicable, the contact details of the data protection officer;

5. the data protection impact assessment provided for in Article 35; and

6. any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

A.2.m Article 49

Official text:

Article 49 outlines the conditions under which personal data can be transferred to a third country or international organization in the absence of an adequacy decision or appropriate safeguards. It provides exceptions and restrictions to protect data subjects and European companies. Official text:

1. [1]In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

    1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

    2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

    3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

    4. the transfer is necessary for important reasons of public interest;

    5. the transfer is necessary for the establishment, exercise or defence of legal claims;

    6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

    7. the transfer is made from a register which according to Union or Member State law 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 a legitimate interest, but only to the extent that the conditions laid

down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. [3]The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. [2]Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

A.2.n Article 14 (5)

Exceptions to BMS providing data subjects information are governed by this Article.

Official text:

a) the data subject already has the information

b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the

conditions and safeguards referred to in **Article 89**(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

A.2.o Article 89

Official text:

Article 89 conditions/safeguards such as applying data minimisation principles, using pseudonymization, documenting any exclusions from certain safeguards, and paying attention to any additional EU Member State legislation related to processing data for research, scientific or public interest purposes. Office text:

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in **Articles 15**,**16**,**18** and **21** subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in **Articles 15**, **16**, **18**, **19**, **20** and **21** subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Appendix B Data Protection Principles

Under the BCRs, any transfer of Personal Data to a third country that does not provide an adequate level of protection must always adhere to the following data protection principles:

B.1 Legal Basis for Processing Personal Data

Personal Data may only be processed under the following conditions:

1) **Consent**: The individual has given clear consent for their personal data to be processed for a specific purpose.

2) **Contract**: The processing is necessary for the performance of a contract with the individual or to take steps to enter a contract.

3) **Legal Obligation**: The processing is necessary for compliance with a legal obligation to which the controller is subject.

4) **Vital Interests**: The processing is necessary to protect the vital interests of the individual or another person.

5) **Public Task**: The 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.

6) **Legitimate Interests**: The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

***Note**: Processing of personal data relating to criminal convictions and offences shall be prohibited, unless the same exemptions as the ones envisaged by Article 10[7] GDPR apply. See here for more information on Article 10.*

B.2 Legal Basis for Processing Sensitive Data

Sensitive Data, particularly Personal Data related to health, may only be processed under the following conditions:

1) **Explicit Consent**: The individual has given explicit consent to the processing of their sensitive data for one or more specified purposes.

2) **Employment, Social Security, and Social Protection Law**: The processing is necessary for carrying out obligations and exercising specific rights of the controller or the data subject in the field of employment, social security, and social protection

[7] Article 10 establishes stringent conditions for processing criminal conviction data, highlighting the necessity for legal authority and protective measures to uphold individual rights.

law, in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law.

3) **Vital Interests**: The processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

4) **Non-Profit Bodies**: The processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim, provided the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and the personal data is not disclosed outside that body without the consent of the data subjects.

5) **Public Data**: The processing relates to personal data which are manifestly made public by the data subject.

6) **Legal Claims**: The processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.

7) **Substantial Public Interest**: The processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8) **Healthcare**: The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services based on Union or Member State law or pursuant to contract with a health professional.

9) **Public Health**: The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

10) **Archiving, Research, and Statistics**: The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1)[8] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[8] Article 89(1) of the GDPR addresses the processing of personal data for specific purposes, including archiving in the public interest, scientific or historical research, and statistical purposes.

B.3 Purpose Limitation

Personal data must be collected for specific, clear, and legitimate purposes and should not be processed further in a manner that is incompatible with those purposes. However, further processing of data for historical, statistical, scientific, or public interest archiving purposes is not considered incompatible if Member States implement appropriate safeguards.

In line with the GDPR provisions, sensitive data can only be processed if additional safeguards are in place.

B.4 Data Quality and Proportionality

Personal Data will be processed fairly, lawfully, and transparently.

The data should be adequate, relevant, and not excessive in relation to the purposes for which it is processed. It must also be accurate and kept up to date when necessary. Reasonable steps should be taken to promptly erase or correct any inaccurate or incomplete data, considering the purposes for which it was collected or further processed.

Personal Data should be retained in a form that allows for the identification of Data Subjects only as long as necessary for the purposes for which the data is processed. Member States must establish appropriate safeguards for Personal Data that is stored for longer periods for purposes such as archiving in the public interest or for historical, statistical, or scientific research.

B.5 Accountability

Entities within BMS that are bound by the BCRs are responsible for ensuring compliance with these Data Protection Principles and must be able to demonstrate this compliance. They must also show that, when processing is based on consent, the Data Subject has given their explicit consent for the processing of their Personal Data.

All BMS entities subject to the BCRs will maintain a written record (including electronic formats) of all processing activities, which must include the following information, and this will made available to all applicable data subjects:

1) The identity and contact details of the Controller and the contact details of the data protection officer

2) The purposes of the processing.

3) The categories of Data Subjects and the types of Personal Data involved.

4) The categories of Recipients to whom the Personal Data has been or will be disclosed, including those in third countries or international organizations.

5) Any transfers of Personal Data to a third country or an international organization, with reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

6) Where possible, the anticipated time limits for erasure of different categories of Personal Data.

7) Where possible, a general description of the Technical and Organizational Security Measures in place.

The record will be made available to the BMS Data Protection Officer (Europe) and the competent Supervisory Authorities on request.

All BMS entities bound by the BCRs will implement appropriate policies to ensure compliance with the BCRs and to effectively incorporate the principles of privacy by design and by default.

B.6 Data Security

BMS entities bound by the BCRs must ensure that data is processed securely, protecting it against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. This will be achieved through appropriate Technical and Organizational Security Measures.

When necessary, BMS entities will conduct Data Protection Impact Assessments (DPIAs) for processing activities that may pose a high risk to individuals' rights and freedoms. If a DPIA indicates that processing could result in a high risk without mitigation measures, the relevant BMS entities will consult the competent Supervisory Authority before proceeding with the processing.

BMS entities will promptly notify the BMS Data Protection Officer (Europe) and the Privacy Law Team of any data breaches. The BMS Data Protection Officer (Europe) and the Privacy Law Team, in collaboration with BMS and/or the EEA entity that reported the breach, will assess the risk associated with the breach. If required, BMS will notify the competent Supervisory Authority. Additionally, BMS will inform affected individuals of a data breach without undue delay when mandated by EU Data Protection law.

BMS will document all data breaches, including details about the incident, its impact, and the remedial actions taken. This documentation will be made available to the competent Supervisory Authority upon request.

B.7 Automated Individual Decisions

Subject to EU Member State and EU Data Protection law, every Data Subject has the right not to be subjected to a decision that has legal effects concerning them or significantly impacts them if that decision is based solely on automated processing of data intended to evaluate certain personal aspects, such as their work performance, reliability, or conduct.

Appendix C Nature and Purposes of Transferred Personal Data

Purposes	Nature of the Personal Data transferred	Data Subject Category
Human resources management Country Transferred to: • Australia • India • United States	► Recruiting ► Payroll ► Benefit and compensation. ► Performance evaluation ► Career development and talent management ► Trainings ► Global directory ► Global reports ► Travel and expenses reimbursement. ► Internal surveys ► Business and Analytics Insights ► Investigations in compliance with local laws and regulations / audit and Sox compliance ► Whistleblowing	Employee and Contractor data
► Communication and relationship management (contacts with healthcare professionals, thought leaders, public authorities, etc.) ► Country Transferred to: • India • United States	► Relationship management activities, medical information delivery, interactions, profiling activities, contractual relationships management, congress, and meetings management, though leader's databases, social media, E-services (e-conferencing etc.) ► Market research activities ► Grants and donation management ► Customers order and shipment	► Healthcare Professionals ► Public Authority Employees ► Third party employees
► Clinical trials / outcome research (observational studies) management ► Country Transferred to: • India • United States	► Sites assessment, selection, evaluation (investigator inclusive) and training, clinical trial implementation and management ► Investigators database (management of investigators recruitment) ► Investigator sponsored trial management. ► Patient recruiting and case report form (inclusive adverse event occurred during clinical trial) ► Patient case reporting	► Healthcare Professionals ► Patients (key-coded) ► Site Staff Personnel
► Pharmacovigilance activities ► • Country Transferred to:	► Management and reports of spontaneous adverse events (SAE) to local and international agencies, affiliates, and marketing authorization owners	► Healthcare Professionals ► Patients (key-coded) ► Employee and Contractors

• India • United States		
► IT support services ► Country Transferred to: • India • United States	► Allocation of software, hardware, electronic tools (company resources) and management of network/application access rights ► Monitoring of company IT resources and other devices use. ► Maintenance and support of applications, systems ► Information security activities	► Employee and Contractors

Appendix D BMS Security Controls

This Section provides information on BMS Security Controls, based on the various standards and controls provided by the National Institute of Standards and Technology (NIST). The

NOTE: The Local Data Controller commits to taking into account any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the Binding Corporate Rules, including measures applied during the transmission and to the processing of the personal data in the country of destination. Some examples are listed below.

Logging	BMS maintains access logs, to ensure recording of access to systems and processes handling personal data.
Access Controls	BMS ensures that appropriate access and revocation controls with periodic managerial reviews when necessary, depending on the nature of processing activities
Confidentiality, Integrity, and Availability	BMS implements, when necessary appropriate NIST Framework controls to ensure confidentiality, integrity, and availability of personal data
Accountability	BMS, in addition to adhering to the NIST Audit & Accountability Controls, demonstrates accountability through a comprehensive Security Training and Awareness Program. This program includes mandatory cybersecurity awareness training for all employees and contractors. Additionally, several other training courses are offered, covering topics such as phishing fundamentals, remote working safety, manufacturing security, and data protection. The Chief Information Security Officer and the Enterprise Learning Services Team (ELS) are responsible for overseeing the training program. They ensure that training is conducted effectively and that compliance with completion requirements is tracked, monitored, and escalated as necessary.
Monitoring	BMS ensures monitoring, security assessment and authorization controls by adopting NIST standards when necessary. BMS also engages in active monitoring to ensure Availability. Security Monitoring, System configuration.

	Security Review - performed at a minimum annually Data Loss Prevention & Monitoring - Designed to detect and prevent potential data breaches, exfiltration transmissions. Appropriate controls are also in place to monitor, detect and/or blocks sensitive data while in use, in motion and at-rest.
System Configuration	BMS adopts appropriate NIST Controls for systems configuration when necessary
Back-Up & Disaster Recovery	BMS ensures appropriate back up controls based on NIST Contingency Planning Controls
Pseudonymization & Encryption	BMS has adopted appropriate identification and Authentication Controls based on NIST framework controls. Application of such controls are dependent on nature of processing activities
Sub-Processor Controls	BMS maintains an enterprise wide Third Party Risk Management (TPRM) standard. Additionally, BMS has a transition document outlining the rollout of its overall TPRM program and the various categories of suppliers and services being utilized. Both documents are reviewed annually by senior management. Under the TPRM framework, critical and major risk third parties are evaluated using an inherent risk questionnaire that generates an inherent risk rating across different security domains. This rating determines the level of assessment required for each supplier. BMS conducts pre-contract due diligence based on individual risk categories, and for certain third parties, background checks are performed by the ethics team. Standard contract templates include requirements related to these areas. Furthermore, BMS conducts periodic assessments of both cybersecurity and physical security. The TPRM framework includes a comprehensive termination and offboarding process, which features a termination checklist that ensures the return of BMS data, revocation of access, and termination of access to systems or facilities. The IT team then confirms that access has been revoked for all users.
Protection in Transit Protection at rest	Commercially available encryption software is used for data in transit and at rest.
Certification	BMS endeavors to create device certifications to limit access to certified users.
Physical Security	BMS maintains physical security standards that addresses the following: Facility access and related electronic access: - Facility intrusion monitoring, detection, and response - CCTV surveillance for sensitive areas - Employee anti-tailgating; and Visitor access controls and logging - Log retention timelines. - Access restrictions for terminated employees

IT security governance and management	BMS maintains a detailed organizational chart as well as defined responsibilities across the Information Security 'Towers'. Each tower has defined roles and responsibilities. Structure IT policies have been created in the following areas: - Access & Password Management; - Business Continuity, - Application Security; - Network Security; - Physical & Environmental Security; - Disaster Recovery; - Asset Management; - Data Classification; - Incident Management; - Third Party Security Management; - Change Management; - Data Encryption; - Configuration Management;

Appendix E BCR Adoption Agreement

This BCR Adoption Agreement (Agreement) is entered into by Bristol-Myers Squibb Pharmaceutical Unlimited Company, whose offices are at Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland, (BMSI) and each BMS entity listed on the signature pages of this Agreement (the BMS Entities).

a) Bristol-Myers Squibb (BMS) and certain other BMS entities entered Binding Corporate Rules to regulate intra-group data transfers from the European Economic Area (EEA) countries to non-EEA countries (Existing BCRs).

b) On or around the date of this Agreement, BMS restated its Binding Corporate Rules to ensure continued compliance with all applicable privacy laws, including the GDPR (Restated BCRs).

c) BMSI and each of the BMS Entities wish to enter into this Agreement to replace the Existing BCRs and formally bind themselves to the Restated BCRs.

The parties agree:

1) This Agreement shall take effect immediately upon approval of the Restated BCRs by the Irish Data Protection Commission (Effective Date).

2) BMSI and each BMS Entity confirms that it has been supplied a copy of the Restated BCRs and, upon execution of this Agreement, hereby agrees that the Existing BCRs shall no longer apply and that it shall be fully bound by all the terms and conditions of the Restated BCRs.

3) Subject to clause 4, if after the Effective Date, a BMS company wishes to be bound by the BCRs (for example, where a new BMS affiliate is created) such BMS company may do so by entering into an accession agreement with BMS in the form set out in the Exhibit to this Agreement (Accession Agreement).

4) Each of the BMS Entities authorizes BMSI on its behalf to take such actions as necessary or required:

   i. To ensure compliance with data protection law.

   ii. In respect of the entering into of an Accession Agreement in accordance with clause 3.

   iii. To terminate this Agreement with respect to a BMS Entity who is no longer a member of the BMS corporate group.

   For clarity, if a BMS Entity enters into an Accession Agreement or is removed from this Agreement in accordance with the foregoing, Appendix E of the Restated BCRs will be updated accordingly without further action of the parties.

5) Subject to clause 4, this Agreement may only be varied in writing with the agreement of each of the parties.

6) This Agreement may be executed in counterparts (which may be exchanged by facsimile or .pdf copies), each of which will be deemed an original, but all of which together will constitute the same Agreement.

7) The provisions of section 6.5 of the Restated BCRs will apply to determine the governing law and jurisdiction.

[signature pages follow]

UNITED STATES OF AMERICA

Bristol-Myers Squibb Company
Company Stamp:
Name: Alejandro Gene
Function: Vice President and Chief Privacy Officer

Signature

_____

Date _____

AUSTRIA

Bristol-Myers Squibb Ges m.b.h
Company Stamp:
Name:
Function:

Signature _____

Date _____

BELGIUM

Bristol-Myers Squibb International Corporation
Company Stamp:
Name:
Function:

Signature _____

Date _____

Bristol-Myers Squibb Belgium S.A.
Company Stamp:
Name:
Function:

Signature _____

Date _____

CZECH REPUBLIC

Bristol-Myers Squibb spol s.r.o
Company Stamp:
Name:
Function:

Signature _____

Date _____

DENMARK

Bristol-Myers Squibb Denmark
Company Stamp:
Name:
Function:

Signature _____

Date _____

FINLAND

Oy Bristol-Myers Squibb (Finland) AB
Company Stamp:
Name:
Function:

Signature _____

Date _____

FRANCE

Bristol-Myers Squibb SARL
Company Stamp:
Name:
Function:

Signature _____

Date _____

BMS Holdings Sarl
Company Stamp:
Name:
Function:

Signature _____

Date _____

Bristol-Myers Squibb EMEA Sarl
Company Stamp:
Name:
Function:

Signature _____

Date _____

GERMANY

Bristol-Myers Squibb GmbH & Co KGaA
Company Stamp:
Name:
Function:

Signature _____

Date _____

GREECE

Bristol-Myers Squibb A.E.
Company Stamp:
Name:
Function:

Signature _____

Date _____

HUNGARY

Bristol-Myers Squibb Kft
Company Stamp:
Name:
Function:

Signature _____

Date _____

IRELAND

Bristol-Myers Squibb Pharmaceutical Unlimited Company
Company Stamp:
Name:
Function:

Signature _____

Date _____

Swords Laboratories
Company Stamp:
Name:
Function:

Signature _____

Date _____

Bristol-Myers Squibb International Company
Company Stamp:
Name:
Function:

Signature _____

Date _____

ITALY

Bristol-Myers Squibb S.r.l.
Company Stamp:
Name:
Function:

Signature _____

Date _____

NETHERLANDS

Bristol-Myers Squibb BV
Company Stamp:
Name:
Function:

Signature _____

Date _____

BMS Pharmaceuticals International Holdings Netherlands B.V
Company Stamp:
Name:
Function:

Signature _____

Date _____

NORWAY

Bristol-Myers Squibb Norway Ltd (Norwegian Branch)
Company Stamp:
Name:
Function:

Signature _____

Date _____

POLAND

Bristol-Myers Squibb Polska SP z.o.o.
Company Stamp:
Name:
Function:

Signature _____

Date _____

Bristol-Myers Squibb Services SP z.o.o..
Company Stamp:
Name:
Function:

Signature _____

Date _____

PORTUGAL

Bristol-Myers Squibb Farmacêutica Portuguesa, S.A
Company Stamp:
Name:
Function:

Signature _____

Date _____

ROMANIA

Bristol-Myers Squibb Marketing Services Srl
Company Stamp:
Name:
Function:

Signature _____

Date _____

SPAIN

Bristol-Myers Squibb S.A.U
Company Stamp:
Name:
Function:

Signature _____

Date _____

SWEDEN

Bristol-Myers Squibb AB
Company Stamp:
Name:
Function:

Signature _____

Date _____

UNITED KINGDOM

Bristol-Myers Squibb Pharmaceuticals UK Limited
Company Stamp:
Name:
Function:

Signature _____

Date _____

Bristol-Myers Squibb Business Services Limited

Company Stamp:
Name:
Function:

Signature _____

Date _____

AUSTRALIA

Bristol-Myers Squibb Australia Pty. Ltd

Company Stamp:
Name:
Function:

Signature _____

Date _____

INDIA

Bristol-Myers Squibb Business Services India Private Limited

Company Stamp:
Name:
Function:

Signature _____

Date _____

Appendix F BCR Accession Agreement

This BCR Accession Agreement (Agreement) is entered into by Bristol-Myers Squibb Pharmaceutical Unlimited Company, whose offices are at Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland, (BMSI) and [*insert*], whose offices are at [*insert*] (Acceding BMS Entity). The background to this Agreement:

a) BMSI and the BMS Entities entered into an agreement to formally adopt and be bound by the Restated BCRs (BCR Adoption Agreement). Pursuant to the BCR Adoption Agreement, each of the BMS Entities authorizes BMSI to enter into this Agreement on each BMS Entity's behalf.

b) The Acceding BMS Entity wishes to formally be bound by the Restated BCRs in accordance with the terms of this Agreement.

The parties agree:

1) The Acceding BMS Entity confirms that it has been supplied a copy of the Restated BCRs and, upon execution of this Agreement, hereby agrees that it shall be fully bound by all the terms and conditions of the Restated BCRs and the Restated BCRs may be enforced by and between BMSI, each of the BMS Entities, and the Acceding BMS Entity.

2) Capitalized terms not defined in this Agreement have the meaning given in the BCR Adoption Agreement.

3) The BCR Adoption Agreement remains in full force and effect.

4) This Agreement may only be varied in writing with the agreement of each of the parties.

5) This Agreement may be executed in counterparts (which may be exchanged by facsimile or .pdf copies), each of which will be deemed an original, but all of which together will constitute the same Agreement.

6) The provisions of section 6.5 of the Restated BCRs shall apply to determine the governing law and jurisdiction.

[signature page follows]

Bristol-Myers Squibb Pharmaceutical Unlimited Company

Company Stamp:
Name:
Function:

Signature _____

Date _____

[Insert name of Acceding BMS Entity]

Bristol-Myers Squibb

Company Stamp:
Name:
Function:

Signature _____

Date _____

Appendix G List of BMS Bound Entities

G.1 Local BMS Data Exporter Located Within The EEA

AUSTRIA	Bristol-Myers Squibb Ges m.b.H Rivergate, Gate 1. 5. 06, Handelskai 92, Vienna, 1200, Austria
BELGIUM	Bristol-Myers Squibb International Corporation Chaussée de la Hulpe, 1170 Brussels, Belgium Bristol-Myers Squibb Belgium S.A. Chaussée de la Hulpe, 1170 Brussels, Belgium
CZECH REPUBLIC	Bristol-Myers Squibb spol. s.r.o Budejovicka 778/3, Prague 4, 140 00, Czech Republic
DENMARK	Bristol-Myers Squibb Denmark, (a branch office of Bristol-Myers Squibb AB), Sverige, Hummeltofevej 49, Virum, 2830, Denmark
FINLAND	Oy Bristol-Myers Squibb (Finland) Ab Tammasaarenkatu 3, Helsinki, FI,00180, Finland
FRANCE	Bristol-Myers Squibb SARL 3, rue Joseph Monier, 92500 Rueil Malmaison France

	BMS HOLDINGS Sarl 3, rue Joseph Monier, 92500 Rueil Malmaison France Bristol-Myers Squibb EMEA Sarl 3, rue Joseph Monier, 92500 Rueil Malmaison, France
GERMANY	Bristol-Myers Squibb GmbH & Co KGaA Arnulfstr. 29, 80636 Muenchen, Germany
GREECE	Bristol-Myers Squibb A.E. 49-53 Attikis str. And 2 Propontidos str. Vrilissia, Athens, 15235, Greece
HUNGARY	Bristol-Myers Squibb Kft Csorsz utca 49-51 fszt., Budapest, 1124, Hungary
IRELAND	Bristol-Myers Squibb Pharmaceuticals Unlimited Company Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland Swords Laboratories Cruiserath Road Mulhuddart, Dublin, 15, Ireland Bristol-Myers Squibb International Company

	Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland
ITALY	Bristol-Myers Squibb S.r.l. Piazzale dell'Industria 40/46, Roma, 00144, Italy
NETHERLANDS	Bristol-Myers Squibb B.V Orteliuslaan 1000, Utrecht, The Netherlands BMS Pharmaceuticals International Holdings Netherlands B.V. Orteliuslaan 1000, Utrecht, The Netherlands
NORWAY	Bristol-Myers Squibb Norway Ltd Lysaker Torg 35, Lysaker, 1366, Norway
POLAND	Bristol-Myers Squibb Polska SP z.o.o. Al. Armii Ludowej 26,00-609 Warsaw Poland Bristol-Myers Squibb Services SP z.o.o.. Al. Armii Ludowej 26, 00-609 Warsaw, Poland

PORTUGAL	Bristol-Myers Squibb Farmacêutica Portuguesa, S.A Edifício Fernão Magalhães, Quinta da Fonte, Porto Salvo, 2780-730 Paço Arcos, Portugal
ROMANIA	BRISTOL MYERS-SQUIBB MARKETING SERVICES SRL Str. Costache Negri nr. 1-5, Opera Center, et. 5, cam. 5.1, 050552 Bucharest District 5, Romania
SPAIN	Bristol-Myers Squibb, S.A.U. Quintanaduenas 6, Madrid, 28050, Spain
SWEDEN	Bristol-Myers Squibb Aktiebolag Gustavslundsvagen 12 SE-16715 Bromma, Sweden

G.2 Local BMS Data Importer Located Outside The EEA

INDIA	**Bristol-Myers Squibb Business Services India Private Limited** 101/102 Flr 1 Kshamalaya, Vitthaldas Thackarsey Marg, Churchgate, Mumbai,400020, India
AUSTRALIA	**Bristol-Myers Squibb Australia Pty. Ltd** 556 Princes Highway, Noble Park, Victoria, 3174, Australia

UNITED STATES OF AMERICA	**Bristol-Myers Squibb Company** Route 206 & Province Line Road, Princeton, New Jersey 08543 United States of America

Appendix H BCR Local Exporter Compliance Check

Here is a sample BCR Compliance Checklist.

1) Assess Legal Basis for Transfer
    - Check with Privacy Law Team and/or the Data Risk Office to ensure assessments are in place for a transfer.
    - Verify the legal basis for the data transfer under GDPR if needed.
    - Ensure data subjects have given explicit consent (if required)
2) Choose an Appropriate Transfer Mechanism
    - Use Standard Contractual Clauses (SCCs) approved by the European Commission for transfers to third parties located outside of the EU/EEA.
    - If internal transfers of personal data to the United States, India or Australia please use Binding Corporate Rules (BCRs)
    - Evaluate the necessity of additional safeguards depending on the nature of the transfer – please consult the Data Risk Office and/or the Privacy Law Team.
3) Check if Transfer Impact Assessment (TIA) is in place for transfer:
    - Assess the legal environment in the US, India, and Australia for any changes in law – please consult the Data Risk Office and the Privacy Law Team.
    - Identify potential risks to data subjects' rights and freedoms.
    - Document the findings and mitigation measures.
4) Implement Technical and Organizational Measures
    - Encrypt data during transfer and at rest.
    - Ensure robust access controls and data minimization practices.
    - Regularly update security measures to address new threats.
5) Review and Update Privacy Notices
    - Ensure privacy notices reflect the data transfer practices.
    - If needed, inform data subjects about the transfer and their rights.
6) Ensure Third-Party Compliance
    - Verify that US-based processors comply with GDPR requirements.
    - Include data protection clauses in contracts with third parties.

7) Monitor and Audit Transfers

- Regularly review data transfer activities.
- Work with the BMS Global Conduct audits to ensure ongoing compliance with GDPR.

8) Maintain Documentation and Records

- Keep detailed records of data transfers and compliance efforts. Please ensure all details recorded in the BMS Records of Processing Activity are up to date – please consult with the Data Risk Office.
- Ensure that all necessary all assessments, decisions, and safeguards implemented are documented correctly and are up to date.

9) Prepare for Data Subject Requests

- Establish procedures for handling data subject access requests (DSARs). Please work with the Data Risk office.
- Ensure data subjects can exercise their rights effectively. Please work with the Data Risk office.

10) Stay Informed and Updated

- Keep abreast of changes in data protection laws and regulations. Maintain regular contact with the Data Risk Office and the Privacy Law Team.
- Update practices and policies as needed to maintain compliance. Contact the Data Risk office if needed.