Bristol-Myers Squibb

Binding Corporate Rules (BCRs)

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

27 October 2023

TABLE OF CONTENTS

1. INTRODUCTION

Bristol-Myers Squibb (BMS) committed its Group in a Process for the adoption of Binding Corporate Rules (BCRs), aimed to regulate intra-group data transfers from European Economic Area (EEA) countries to non-EEA countries, and hereby provides a restatement of its BCRs to ensure continued compliance with all applicable privacy laws including the GDPR.

This agreement is a full part of the proactive policy with regard to data privacy that Bristol-Myers Squibb has followed for many years. To date, BMS has an internal organization which integrates Data Protection Principles (see in Appendix 2) in its whole decision making process, in accordance with the provisions of the GDPR and the 2002/58 EU Directive. This organization singularizes itself through the existence, at a worldwide level, of a Data Risk Office (privacy operations), a global Privacy Law Team (advisory), a Data Protection Officer all working in conjunction with the wider BMS business and IT teams, including a network of local in-country "Data Protection Advisers" and legal teams. It is the in-country teams that are responsible for enforcing, at local level, all defined guidelines, policies and procedures relating to data protection issues. The importance of privacy and confidentiality principles is also highlighted in our Standards of Business Conduct and Ethics.

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

In this context, the decision to adopt BCRs is one step further toward a full commitment to data protection compliance. Beyond providing adequate protection for the transfer of Personal Data outside the EEA, this approach aims to optimize the broadcasting and sharing of our culture on privacy within our Group in order to enhance this commitment to all of our stakeholders, partners and/or interlocutors. With regard to the scope of our BCRs, appropriate entities and employees of the Group shall comply with the following guidelines, as well as with applicable local laws.

Bristol-Myers Squibb Pharmaceutical Unlimited Company (BMSI), whose offices are at Plaza 254, Blanchardstown Corporate Park 2, Ballycoolin, Dublin, 15, Ireland, a subsidiary of BMS, 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. BMSI as the Head Controller, to ensure continued compliance with all applicable privacy laws and in anticipation of the effective date of the GDPR, has appointed the EU Data Protection Officer (DPO) and the Privacy Law Team for supervising, at global level, the implementation of the BCRs in all appropriate BMS entities. BMSI is best placed to enforce the BCRs within the Group and the EU DPO team is based in Dublin, Ireland.

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

Would a violation of the BCRs be established, any corrective measure (legal 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, the Office of the EU DPO, the Office of Compliance and Ethics, the Local Data Controller or the Local Data Protection Officer.

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs are defined in Appendix 1, provided that these terms and expressions shall always be interpreted according to the GDPR and the 2002/58 EU Directive.

2.2. DATA PROTECTION PRINCIPLES

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

- **Legal basis for Processing Personal Data and Sensitive Data**: Personal Data and Sensitive Data shall only be Processed under the conditions defined in the GDPR.

- **Purpose limitation**: Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a way incompatible with those purposes or as otherwise permitted by the GDPR.

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

- **Transparency**: Personal Data shall always be collected and further Processed on a transparent basis (see paragraph 4.1)

- **Data Subject rights**: Data Subjects are entitled to exercise their legal rights in respect of their Personal Data BMS holds (see paragraph 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 paragraph 4.3).

- **Security and confidentiality**: appropriate Technical and Organizational Security Measures shall be implemented to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing (see paragraph 4.5).

3. SCOPE OF THE BCRs

3.1. GEOGRAPHICAL SCOPE

The BCRs apply to Personal Data Processed within the EEA and transferred outside the EEA.

3.2. MATERIAL SCOPE

The nature and purposes of the Personal Data being transferred within the scope of the BCRs is detailed in Appendix 3.

3.3. CORPORATE SCOPE

The BCRs shall become binding on the BMS entities who are a party to the BCR Adoption Agreement set out in Appendix 4. Appendix 5 gives a list of all BMS entities bound by the BCRs.

4. EFFECTIVENESS OF THE BCRs

4.1. TRANSPARENCY AND INFORMATION RIGHT

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

1. The BCRs shall always be readily available to every Data Subject and therefore shall be uploaded both on BMS intranet and internet corporate website. Furthermore, a Data Subject will always be able to obtain, upon request, a copy of the BCRs from the Data Risk Office and/or the Local Data Controller.

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

Local Data Protection Officers, in coordination with the Office of the EU DPO, and the Privacy Law Team, shall be able to provide templates of notices to every Local Data Controller within the Group, for any purpose that requires information to be made to the Data Subjects.

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

a) the identity of the Controller(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;

b) the nature and purposes of the Processing for which the data are intended as well as the legal basis for the Processing; to the extent Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal; to the extent Processing is based on legitimate interests, the legitimate interest pursued;

c) when appropriate, the purpose(s) of the transfer(s) outside the EEA and the mechanisms used to effect such transfer(s) (including the BCRs);

d) any further information such as:

- the categories of data concerned;
- the Recipients or categories of Recipients of the data;
- the period for which data will be retained, or if that is not possible, the criteria used to determine that period;
- whether replies to the questions are obligatory (under contract or statute) or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to, rectification of, erasure of, portability of the data concerning him as well as the right to restrict or object to the Processing of data concerning him, and the right to lodge a complaint with a Supervisory Authority;
- if applicable, from which source the data originated and whether it came from publicly accessible sources; and
- any further information which might be necessary in order to ensure that the Processing is made in a transparent manner (e.g. Processing through automated decision-making).

Where, with regard to an existing data Processing, a new purpose or a new category of Recipient arise, the appropriate notice of information shall be consequently modified and the Data Subjects shall be informed.

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

According to Article 14.5 of the GDPR, the above-mentioned information will exceptionally not need to be provided where:

a) the Data Subjects already have this 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) of the GDPR or in so far as the obligation to provide information is likely to render impossible or seriously impair the achievement of the objectives of that Processing; in such cases BMS 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, which provides appropriate measures to protect the Data Subject's legitimate interests; and

d) where the information must remain confidential subject to an obligation of professional secrecy regulated by law, or if obtaining or disclosure is expressly laid down by law (see paragraph 6.1).

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. Thus:

1. Every Data Subject has the right to obtain from BMS:

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

- confirmation as to whether or not data relating to him are being Processed and information at least as to the purposes of the Processing; the categories of data concerned; the Recipients or categories of Recipients to whom the data are disclosed; where possible, the envisaged period for which the Personal Data will be stored or the criteria used to determine that period; the existence of the rights of rectification, erasure, restriction of Processing and objection to Processing; the right to lodge a complaint with a Supervisory Authority; and the existence of automatic decision making;

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

b) as appropriate the rectification, erasure or blocking of Personal Data to the extent that the Processing does not comply with the provisions of the BCRs, in particular because of the incomplete or inaccurate nature of the data;

c) as appropriate, to object to the Processing of data relating to him at any time on compelling legitimate grounds relating to their particular situation and where data are Processed for direct marketing purposes; and

d) to request the portability of data relating to him.

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

2. 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:

   a) the Personal Data are no longer necessary for the purposes for which they were collected or otherwise Processed;

   b) the Data Subject withdraws his/her 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;

   c) 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;

   d) the Personal Data have to be erased for compliance with a legal obligation in Union or Member State law, including where a court or regulatory authority has ruled that the data concerned must be erased; or

   e) the Personal Data has been unlawfully Processed.

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

   a) exercising the right of freedom of expression and information;

   b) compliance with a legal obligation which requires Processing Union or pursuant to Member State law;

   c) reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the GDPR;

   d) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 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; or

   e) the establishment, exercise or defence of legal claims.

In the event that one of the above applies, BMS will communicate any rectification or erasure carried out to the BMS entity and/or third parties to whom the data have been transferred, unless this proves impossible or involves a disproportionate effort, and will inform the Data Subjects about those Recipients upon request.

1. Every Data Subject shall be clearly informed, in accordance with paragraph 4.1, on how he can exercise their rights.

2. Specific guidelines and procedures shall be in place within the Group, at the local level, to ensure the exercise of the rights specified above. In particular,

all BMS employees shall be trained to recognize a Data Subject rights request. Each request shall be acknowledged and handled according to the local procedure in place. A specific answer, given within one month of receipt of the request, shall be systematically given to the Data Subject. Taking into account the complexity and number of the requests, that one month period may be extended up to a maximum of two further months, in which case the Data Subject should be informed accordingly. If the request is found legitimate, BMS shall take any necessary steps to handle the matter in due times. If the request is denied, the reason for denial shall be communicated in writing to the Data Subject. In such a case, the Data Subject may follow the internal complaint mechanism specified in paragraph 4.4.

3. Local Data Protection Officers, in coordination with the Office of the EU DPO and the Privacy Law Team, shall always be at the disposal of both Local Data Controllers and Data Subjects to provide any help.

4.3. AUTOMATED INDIVIDUAL DECISIONS

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

4.4. INTERNAL COMPLAINT MECHANISM

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

1. Specific guidelines and procedures shall be in place within the Group, at the local level, to ensure a complaint mechanism to be consistent and to ensure sufficient information to be provided to the Data Subjects about these procedures. Data Subjects may bring questions or complaints through a dedicated email address (eudpo@bms.com) or other available contact points. The complaints shall be dealt, according to each category of Data Subjects involved (i.e. employees, healthcare professionals, etc.), by a clearly identified local department or by the local Data Protection Officer.

    a) Employees can bring questions or complaints about the Processing of their Personal Data to BMS' designated privacy contacts at eudpo@bms.com.

    b) Healthcare professionals can bring questions or complaints about the Processing of their Personal Data to BMS' designated privacy contacts at eudpo@bms.com.

    c) Other Data Subjects can bring questions and complaints about the Processing of their Personal Data to BMS' designated privacy contacts at eudpo@bms.com.

2. The ones in charge of handling a claim shall benefit from an appropriate level of independence in the exercise of their duties. When a complaint is registered, it must be dealt with without undue delay and in any event within one month of the complaint being made. If the circumstances are complex and the complaint cannot be resolved within one month, the period may be extended by a maximum of two months.

3. If the Data Subject or BMS representatives cannot resolve the claim at the local level, the complaint handling mechanism shall allow for escalation of the problem through the Data Risk Office who will in turn communicate the complaint to the Office of Compliance and Ethics, Office of the EU DPO, and the Privacy Law Team. The escalation process must occur within a reasonable period of time to ensure that the complaint is handled within the timeframe indicated in the paragraph above.

4. Data Subjects will be informed of the remediation measures taken by BMS entities, if any, and as appropriate. Data Subjects who are not satisfied with the decision taken or the measures proposed in response to their complaint, can file a complaint with the competent Supervisory Authorities or commence a legal action before the competent courts as indicated in paragraphs 5.2 and 5.3.

5. Each Local Data Controller and Local Data Privacy Officer shall regularly report to the Office of the EU DPO about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of privacy compliance.

6. Complaints will be handled in good faith together with the Data Subject. All BMS representatives and employees shall, at the local level, do their best efforts to help the Local Data Controller or the Local Data Privacy Officer to settle a complaint.

Nothing in the BCRs prevents individuals at any time from bringing complaints for violations of the BCRs to competent Supervisory Authorities or from commencing a legal action before courts of competent jurisdiction.

4.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

Ensuring that personal information is appropriately protected from data breaches is a BMS top priority. Thus, each Local Data Controller shall implement appropriate Technical and Organizational Security Measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the data to be protected.

Consequently, appropriate information security policies and procedures shall be designed and implemented within the Group. These security policies set up all appropriate physical and

logical measures with a view to prevent or deter accidental destruction, modification or unauthorized disclosure or access to Personal Data. These policies and procedures shall be regularly audited (see paragraph 4.8).

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

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

3. Each Local Data Controller will notify without undue delay any data breaches to the Office of the EU DPO. The Office of the EU DPO in cooperation with the Privacy Law Team and the Head Controller and/or the Local Data Controller having reported the data breach, will determine the risk posed by the data breach, and BMS will notify the competent Supervisory Authority within 72 hours of becoming aware of the breach, unless the data breach is unlikely to result in a risk to the rights and freedoms of the affected Data Subjects. BMS will notify affected customers and employees of a data breach without undue delay where the data breach is likely to result in a high risk to the rights and freedoms of Data Subjects. BMS will document data breaches (including the facts relating to the data breach) and will make the documentation available to the competent Supervisory Authority on request (as further detailed in the Data Protection Principles in Appendix 2).

Where a Local Data Controller requests that another BMS entity undertakes Processing of Personal Data on its behalf, the following safeguards shall be followed:

1. Where the data Processing is carried out, the Local Data Controller shall choose a Processor providing sufficient guarantees in respect of the Technical and Organizational Security Measures governing the Processing to be carried out, and must ensure compliance with those measures. The appointed BMS entity shall undertake in writing to provide those sufficient guarantees. Local Data Protection Officers, in coordination with the Office of the EU DPO, and the Privacy Law Team, shall be able to provide templates of the appropriate clauses that satisfy the requirements arising under Article 28(3) of the GDPR to a Local Data Controller within the Group.

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

3. Upon termination of the work to be done, the appointed entity shall undertake to delete all the data transferred or, if any legal data retention requirement is applicable, to keep it recorded, provided that appropriate Technical and Organizational Security Measures are taken to protect Personal Data against accidental or unlawful form of Processing.

4.6. ACCOUNTABILITY

BMS entities bound by the BCRs shall be responsible for, and be able to demonstrate compliance with, Data Protection Principles. Thus:

1. Each entity shall maintain a record in writing (including in electronic form) of all Processing activities. The competent Supervisory Authorities shall receive a copy of the record of Processing activities upon request.

2. A data protection impact assessments shall be carried out for Processing activities that present high risks to the rights and freedoms of Data Subjects.

3. When Processing is based on Consent, each entity relying on that Consent shall be able to demonstrate that the Data Subject has Consented to Processing of their Personal Data.

4. All BMS entities bound by the BCRs will maintain appropriate policies to facilitate compliance with the BCRs and to ensure appropriate consideration of the principles of privacy by design and by default.

4.7. TRAINING PROGRAMS

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

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

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

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

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

5. At local level, each Controller and/or Data Privacy Officer/Privacy Law Team shall feel free to enhance the privacy training programs described above by adding any appropriate training material.

6. Privacy training programs shall be reviewed and approved by experienced BMS officers, in coordination with the Local Data Privacy Officers, the Office of the EU DPO, and the Privacy Law Team. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.8).

4.8. AUDIT PROGRAM

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

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

2. Data protection audits shall be decided directly by the Compliance / Audit Departments or upon specific request of the Head Controller, the Office of Compliance and Ethics, a Local Data Controller, a Local Data Privacy Officer, the Office of the EU DPO, or the Privacy Law Team. The ones in charge of handling an audit will always benefit from an appropriate level of independence in the exercise of their duties.

3. The results of all audits shall be communicated to the officers of BMSI, the Office of the EU DPO, the Data Risk Office and/or the Local Data Protection Officer and/or the local Controller.

4. The competent Supervisory Authorities shall receive a copy of such audit upon request. Each Local Data Controller shall accept to be audited by a competent Supervisory Authority and to abide by the advice of a competent Supervisory Authority on any issue related to the BCRs.

5. As provided by paragraph 5.1.3 below, Local Data Privacy Officers, in coordination with the Office of the EU DPO, and the Privacy Law Team, shall report every year to the Head Controller about all the actions and measures taken with regard to data protection issues (training programs, inventory of Personal Data Processing implemented, management of complaints, etc.). Furthermore, each Local Data Privacy Officer shall take every necessary step to make sure that Local Data Controllers comply with the provisions of the BCRs. To this end, a “BCR compliance check list” shall be used at local level to make compliance checks.

6. The Office of the EU DPO shall also regularly report to the Head Controller about the implementation of the BCRs within each Local Data Controller.

7. Thanks to the audit results and the reports mentioned above, the Head Controller and/or the Office of the EU DPO and/or the Privacy Law Team shall decide any appropriate legal measures, or Technical and Organizational Security Measures in order to improve data protection management within the Group, both at global and/or local level.

5. BINDING NATURE OF THE BCRs

5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE

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

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

Compliance with those guidelines and procedures rely on training programs and auditing activities for all our employees, on a day to day basis. The importance of privacy and confidentiality principles is also highlighted in our Standards of Business Conduct and Ethics.

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

At local level, each local Data Privacy Officer shall be responsible for the implementation of the BCRs. Thus:

1. Each entity shall take every necessary step to make sure that Local Data Controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check list" shall be used at local level to make compliance checks. Data protection audits decided by the Compliance / Audit Departments, the Office of the EU DPO or the Privacy Law Team may focus on how these compliance checks are made at local level.

2. Local Data Protection Officers, in coordination with the Office of the EU DPO and the Privacy Law Team, shall always be at the disposal of both Local Data Controller and Data Subjects to provide any help with regard to a data protection issue, especially the BCRs.

3. The Local Data Privacy Officers, in coordination with the Office of the EU DPO and the Privacy Law Team, shall report every year to the Head Controller about all the actions and measures taken with regard to data protection issues (training programs, inventory of Personal Data Processing implemented, management of complaints, etc.), especially the implementation of the BCRs.

4. Each Local Data Controller and Local Data Privacy Officer shall regularly report to the Office of the EU DPO and the Privacy Law Team about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of privacy.

5. Local Data Protection Officers, in coordination with the Office of the EU DPO and the Privacy Law Team, shall be able to provide any appropriate templates (i.e. notices of information, clauses, etc.) to each Local Data Controller within the Group for any purpose related to a data protection issue.

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

1. The Office of the EU DPO and the Privacy Law Team shall 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 Compliance / Audit Departments or upon specific request of a Local Data Privacy Officer, the Office of Compliance and Ethics, the Office of the EU DPO or the Privacy Law Team. The results of all audits or reports shall be communicated to the Data Protection Office, the Office of the EU DPO and the Privacy Law Team.

3. Thanks to the audit results and the reports mentioned above, the Head Controller, the Office of Compliance and Ethics, the Data Risk Office, the Privacy Law Team, the Office of the EU DPO, a Local Data Controller or a Local Data Privacy Officer shall decide any appropriate measure in order to improve data protection management within the Group, both at global and/or local level.

4. If a violation of the BCRs is established, any 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 EU DPO, a Local Data Controller or a Local Data Protection Officer, in coordination with the Office of Compliance and Ethics.

5. Privacy training programs shall be reviewed and approved by BMS senior officers, in coordination with the Privacy Law Team, the Office of the EU DPO and Local Data Privacy Officers. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.8).

5.2. THIRD PARTY BENEFICIARY RIGHTS

A Data Subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs, and in particular paragraphs 2.2, 4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 5.5, 6.1, 6.2, 6.5, and Appendix 2. Thus:

1. Each Data Subject shall have the right to take its case, at its best convenience, to the competent Supervisory Authority (i.e. located in the Data Subject's country of habitual residence, their place of work, or the place of the alleged infringement) or before the competent court (i.e. located in the EU country where BMS has an establishment or the Data Subject's EU country of habitual residence), for any breach of the BCRs.

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

3. The BCRs shall always be readily available to every Data Subject, in the conditions described in paragraph 4.1. Furthermore, a Data Subject shall

always be able to obtain, upon request, a copy of the BCRs from the Local Data Protection Officer, the Local Data Controller, EU DPO, or the Privacy Law Team.

5.3. LIABILITY

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

1. Each Local Data Exporter agrees to oversee the relevant Local Data Importer's compliance with these BCRs. The Local Data Exporter accepts responsibility for violations of these BCRs by Local Data Importers and agrees to take the necessary actions to remedy the acts of Local Data Importers and to pay any compensation for material and non-material damages awarded to Data Subjects by the courts mentioned in paragraph 5.2, unless the relevant Local Data Importer has already paid the compensation or complied with the court order in question. The Local Data Exporter shall therefore have sufficient financial resources at their disposal to cover the payment of compensation for breach of the BCRs. Unless prohibited by the relevant European Union or Member State law, liability as between the Local Data Importer and Local Data Exporter shall be limited to actual material and non-material damage suffered and indirect or punitive damages shall be specifically excluded.

2. The burden of proof shall stay with each Local Data Exporter to demonstrate that the entity outside the EEA that received Personal Data from the Local Data Exporter is not liable for the violation resulting in the damages claimed by the Data Subject. The Local Data Exporter may be exempted from any liability, in whole or in part, if it is proved that the entity outside the EEA is not responsible for the event giving rise to the damage.

3. If a violation of the BCRs is established, any correction 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) shall be taken on the initiative of the Head Controller, the Data Risk Office, the Privacy Law Team, the Office of the EU DPO, the Local Data Controller or the Local Data Protection Officer.

5.4. SANCTION

Would a violation of the BCRs, either by Local Data Controller representatives or employees, be established, any appropriate disciplinary sanction or judicial action may occur, in accordance with local labour law, on the initiative of the Head Controller, the Data Protection Office, the Privacy Law Team, the Office of the EU DPO, the Local Data Controller or the Local Data Protection Officer, in coordination with the Office of Compliance and Ethics.

Thus, each Local Data Controller and Data Privacy Officer shall pay specific attention to any audit results (see paragraph 4.8) establishing non-compliance issues against representatives or employees, especially in case of:

1. noncompliance with the Data Protection Principles set out in paragraph 2.2 and Appendix 2;

2. noncompliance with guidelines or procedures relating to the exercise of the rights specified in paragraph 4;

3. noncompliance with security policies designed to implement appropriate Technical and Organizational Security Measures to protect Personal Data; or

4. noncompliance with training programs designed to raise employee's awareness on data protection issues.

5.5. MUTUAL ASSISTANCE AND COOPERATION WITH SUPERVISORY AUTHORITIES

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

1. The competent Supervisory Authorities shall receive, upon request, an updated copy of the BCRs or all related procedures, policies, guidelines or training materials specified in paragraph 4.7.

2. The Local Data Controller shall reply within a reasonable period of time to any request addressed by a competent Supervisory Authority, including audit requests.

3. The Local Data Controller shall apply any relevant recommendation or advice from a competent Supervisory Authority relating to the implementation of the BCRs.

4. The Local Data Controller shall abide by a decision of a competent Supervisory Authority, related to the implementation of the BCRs, against which no further appeal is possible before competent courts.

5. The Office of the EU DPO or the Privacy Law Team shall be at the disposal of the competent Supervisory Authorities for any matter related to the implementation of the BCRs.

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

6. FINAL PROVISIONS

6.1. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

BMS undertakes that appropriate entities and employees of the Group shall comply with the provisions of the BCRs, as well as with the provision of the EU Directive 2002/58 and applicable local laws, as provided by Article 47 of the GDPR.

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

BMS undertakes to verify that it has no reason to believe the laws and practices applicable to the Processing of Personal Data by Local Data Importers in third countries, including any requirement to disclose Personal Data or measures authorizing access by public authorities, prevent Local Data Importers from fulfilling their obligations under these BCRs. In addressing this obligation and before any transfers of Personal Data (including data in transit), BMS undertakes to conduct an assessment, which takes due account of: (i) the specific circumstances of the transfers; (ii) the laws and practices of the third countries of destination (relevant in light of the specific circumstances of the transfers, and the applicable limitations and safeguards); and (iii) the relevant contractual, Technical and Organizational Security Measures put in place under these BCRs, including measures applied during transmission and to the Processing of the Personal Data in the country of destination. Local Data Importers will make best efforts to provide relevant information to assist with this assessment, which BMS shall document and make available to the competent Supervisory Authority upon request. BMS will not transfer data using these BCRs until the relevant transfer assessments have been made and that all members to the BCR are confident that their obligations outlined in these BCRs can be met.

If BMS becomes aware that a Local Data Importer can no longer fulfil its obligations under these BCRs, the Local Data Importer will promptly notify the Local Data Exporter; BMS shall promptly identify appropriate supplementary measures to be adopted by the Local Data Exporter and/or Local Data Importer to address the situation.

Where there is a conflict between national law and the commitments in the BCR, the Local Data Privacy Officer and the Local Data Controller, in coordination with the Office of the DPO or the Privacy Law Team, shall decide on what action to take and will consult the competent Supervisory Authority in case of doubt. The Local Data Exporter shall suspend the transfer if BMS considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent Supervisory Authority to do so. Following such a suspension, the Local Data Exporter can choose to end the transfer (or set of transfers) and to request that any Personal Data transferred prior to the suspension held by the Local Data Importer be returned to the Local Data Exporter or the Personal Data destroyed or deleted in its entirety.

In case that any BMS entity subject to the BCRs considers that any provision of applicable local law it is subject to in any non-EEA country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, it will promptly inform the Office of the EU DPO and the Privacy Law Team, and BMSI will report the issue to the competent Supervisory Authority (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). This includes any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body, as well as any direct access by such authorities to Personal Data transferred under these BCRs. In such a case, the competent Supervisory Authority will be provided with information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited under applicable law). In cases where suspension and/or notification of such a request are prohibited, BMSI will use and document best efforts to obtain a right to waive that prohibition in order to communicate as much information as it can and as soon as possible. In cases where, despite having used best efforts, BMSI is unable to notify the competent Supervisory Authority, it shall annually provide to competent Supervisory Authorities general information on the requests it has received.

BMS shall assess the legality of a request for disclosure as described above – in particular, whether it is within the powers granted to the requesting public authority – and challenge the

request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and/or principles of international comity. BMS shall, under the same conditions, pursue possibilities of appeal. When challenging a request, BMS shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. BMS shall document its legal assessment and any challenge to the request for disclosure, and to the extent permissible under the laws of the country of destination, make the documentation available to the competent Supervisory Authority on request. BMS shall not disclose the Personal Data requested until required to do so under the applicable procedural rules, and shall provide the minimum amount of information permissible when responding, based on a reasonable interpretation of the request.

If the relevant BMS entity is required by applicable law to make transfers of Personal Data to public authorities, those transfers will not go beyond what is necessary in a democratic society and cannot be massive, disproportionate and indiscriminate.

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

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

1. External Processors located inside the EEA or in a country recognised by the EU Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the Processor shall act only on instructions from the Controller and shall be responsible for the implementation of the adequate security and confidentiality measures (see paragraph 4.5). Local Data Protection Officers, in coordination with the Office of the EU DPO and the Privacy Law Team, shall be able to provide appropriate templates of the appropriate clauses to a Local Data Controller within the Group.

2. All transfers of Personal Data to external Controllers located out of the EEA must respect the European rules on transborder data flows (Articles 44-50 of the GDPR), 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 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 (Articles 28-29 of the GDPR) in addition to the rules on transborder data flows (Articles 44-50 of the GDPR), 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. UPDATES OF THE BCRs

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

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

BMS undertakes that appropriate information will be given, once a year and without undue delay, to all BMS entities bound by these BCRs, the Data Subjects, the appropriate Local Data Controllers and the competent Supervisory Authorities about any update with a brief explanation of the changes. Any changes to the BCRs that could significantly affect the BCRs or possible affect the level of protection offered by them will be communicated promptly to the competent Supervisory Authority.

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

6.4. DEROGATIONS OF ARTICLE 49 OF THE GDPR

Nothing in these BCRs shall be understood to prejudice BMS' ability to rely upon alternative data transfer mechanisms provided for under the GDPR, where applicable. In accordance with Article 49 of the GDPR and applicable local law, a transfer or a set of transfers of Personal Data to a third country which does not ensure an adequate level of protection may take place from a Local Data Controller on condition that:

- the Data Subject has given their Consent unambiguously 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;

- 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 in response to the Data Subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and a third party;

- the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims;

- 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; or

- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

6.5. APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

The BCRs shall be adopted by the Head Controller, in coordination with the Data Risk Office, the Privacy Law Team and the Office of the EU DPO.

In the event that a Local Data Controller would be found in substantial or persistent breach of the terms of the BCRs, the Head Controller may temporarily suspend the transfer of Personal Data until the breach is repaired. Should the breach not be repaired in due times, the Head Controller shall terminate the BCR in respect of the relevant Local Data Controller. In such a case, the Local Data Controller shall take every necessary step in order to respect the European rules on transborder data flows (Articles 44-50 of the GDPR), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

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

Jurisdiction shall be attributed in accordance with paragraph 5.2 and 5.3.

In case of contradiction between the BCRs and the Appendices, the BCRs shall always prevail. In case of contradiction between the BCRs and other global or local policies, procedures or guidelines, the BCRs shall always prevail. In case of contradiction or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the GDPR and the 2002/58 EU Directive.

APPENDICES

- **Appendix 1 – Definitions**
- **Appendix 2 – Data Protection Principles**
- **Appendix 3 – Nature and purposes of the personal data being transferred within the scope of the BCRs**
- **Appendix 4 – BMS Security Controls**
- **Appendix 5 - BCR Adoption Agreement**
- **Appendix 6 – List of BMS entities bound by the BCRs**

APPENDIX 1

DEFINITIONS

The terms and expressions used in the BCRs are defined in this Appendix, provided that these terms and expressions shall always be interpreted according to the GDPR and the 2002/58 EU Directive.

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

"**Consent**" shall mean any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies their agreement to Personal Data relating to him or her being Processed.

"**Controller**" shall mean 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**" shall mean the internal privacy operations team and governance body overseen by the BMS EU Data Protection Officer, and comprised of a network of DPO liaisons, including global business function leads, local country specific DPOs and other relevant BMS teams. It also includes a DRO Operations team that lends support through ongoing monitoring and sustaining the DRO processes, such as breach notification reporting, data subject requests, third-party assessments, data protection impact assessments, records of processing, training and awareness.

"**EU DPO/EU Data Protection Office**" shall mean the EU Data Protection Officer, responsible for monitoring compliance with the GDPR, and other EU and Member State provisions relating to data protection, and the BCRs.

"**GDPR**" shall mean 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 (General Data Protection Regulation)'.

"**Privacy Law Team**" shall mean 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.

"**Group**" means BMS and its affiliates from time to time.

"**Head Controller**" shall mean Bristol-Myers Squibb Company located in the US, Route 206 & Province Line Road, Princeton, New Jersey 08543, which alone or jointly with others determines the purposes and means of the Processing of Personal Data and which is in charge of the formal adoption of BCRs to be implemented within the Group.

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

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

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

"**Local Data Protection Officer**" shall mean an experienced BMS officer within a Local Data Controller who is responsible for managing business awareness and compliance with Applicable Data Protection Law and BMS privacy policies, procedures and guidelines, especially the BCRs.

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

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

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

"**Processor**" shall mean a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Controller.

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

"**Sensitive Data**" shall mean Personal Data revealing directly or indirectly racial or ethnic origin, political opinions, philosophical or religious beliefs, or trade union membership; genetic data or biometric data Processed for the purpose of uniquely identifying a natural person; or Personal Data related to the health, sex life or sexual orientation of individuals.

"**Supervisory Authority**" shall mean an independent public authority which is established by a Member State pursuant to GDPR Article 51.

"**Technical and Organizational Security Measures**" shall mean measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

APPENDIX 2

DATA PROTECTION PRINCIPLES

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

LEGAL BASIS FOR PROCESSING PERSONAL DATA

Personal Data shall be Processed only if:

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

LEGAL BASIS FOR PROCESSING SENSITIVE DATA

Sensitive Data, especially Personal Data concerning health, shall be Processed only if:

- the Data Subject has given their explicit Consent to the Processing of those Sensitive Data, except where the applicable laws prohibit it;
- the Processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards;
- the Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving their Consent;
- the Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the Consent of the Data Subjects;

- the Processing relates to Sensitive Data which is manifestly made public by the Data Subject;

- the Processing of Sensitive Data is necessary for the establishment, exercise or defence of legal claims;

- the Processing is necessary for reasons of substantial public interest, on the basis of European 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;

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

- 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 health care and of medicinal products or medical devices, on the basis of European 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; or

- the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on European 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.

PURPOSE LIMITATION

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

In accordance with the provisions of the GDPR, Sensitive Data shall only be Processed with additional safeguards.

DATA QUALITY AND PROPORTIONALITY

Personal Data shall be Processed fairly, lawfully and in a transparent manner.

Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed; accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further Processed, are erased or rectified without delay.

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data are Processed. Member States shall lay down appropriate safeguards for Personal Data stored for longer periods for archiving in the public interest, or for historical, statistical or scientific use.

ACCOUNTABILITY

BMS entities bound by the BCRs shall be responsible for, and be able to demonstrate compliance with, these Data Protection Principles. They shall also be able to demonstrate that, when Processing is based on Consent, the Data Subject has Consented to Processing of their Personal Data.

All BMS entities bound by the BCRs will maintain a record in writing (including in electronic form) of all Processing activities, including the following information:

- the identity and the contact details of the Controller;
- the purposes of the Processing;
- the categories of Data Subjects and of the categories of Personal Data;
- the categories of Recipients to whom the Personal Data have been or will be disclosed including Recipients in third countries or international organizations;
- transfers of Personal Data to a third country or an international organization;
- where possible, the envisaged time limits for erasure of the different categories of Personal Data; and
- where possible, a general description of the Technical and Organizational Security Measures in place.

The record will be made available to the EU DPO and competent Supervisory Authorities on request.

All BMS entities bound by the BCRs will maintain appropriate policies to facilitate compliance with the BCRs and to ensure appropriate consideration of the principles of privacy by design and by default.

DATA SECURITY

BMS entities bound by the BCRs shall ensure that data is Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate Technical and Organizational Security Measures.

When required, the BMS entities bound by the BCRs will carry out data protection impact assessments (DPIAs) for Processing operations that are likely to result in a high risk to the rights and freedoms of individuals. Where a DPIA indicates that the Processing would result in a high risk in the absence of measures taken to mitigate the risk, the relevant BMS entities will consult the competent Supervisory Authority, prior to Processing.

BMS entities bound by the BCRs will notify without undue delay any data breaches to the Privacy Law Team. The Privacy Law Team in cooperation with BMS and/or the EEA entity having reported the data breach, will determine the risk posed by the data breach, and BMS will notify the competent Supervisory Authority if required under applicable law. BMS will notify affected individuals of a data breach without undue delay where required under applicable law. BMS will document data breaches (including the facts relating to the data breach, its effects and the remedial action taken), and will make the documentation available to the competent Supervisory Authority on request.

AUTOMATED INDIVIDUAL DECISIONS

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

APPENDIX 3

NATURE AND PURPOSES OF PERSONAL DATA BEING TRANSFERRED WITHIN THE SCOPE OF THE BCRs

Purposes	Nature of the Personal Data transferred
► Human resources management	► 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
► Communication and relationship management (contacts with healthcare professionals, thought leaders, public authorities, etc.)	► Relationship management activities, medical information delivery, interactions, profiling activities, contractual relationships management, congress and meetings management, though leaders databases, social media, E-services (e-conferencing etc.) ► Market research activities ► Grants and donation management ► Customers order and shipment
► Clinical trials / outcome research (observational studies) management	► 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
► Pharmacovigilance activities	► Management and reports of spontaneous adverse events (SAE) to local and international agencies, affiliates and marketing authorization owners
► IT support services	► 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

APPENDIX 4

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).

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 following the NIST Audit & Accountability Controls, demonstrates accountability through robust Security Training and Awareness Program which includes mandatory Cybersecurity awareness training required for all employees and contractors. There are also several other training courses available including, but not limited to, phishing fundamentals, remote working safety, manufacturing security, data protection. The Director of Cyber Governance, along with the Training and Awareness manager, are responsible for ensuring the training is conducted and that compliance to completion is tracked, monitored, and escalated as needed.
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
Psuedonymisation & 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 standard. In addition, BMS maintains a transition document on how the enterprise is rolling out an overall Third Party Risk Management program and different categories of suppliers/services that are being used. Both documents are reviewed by senior management on an annual basis. Under Third Party Risk Management, critical and major risk third parties are assessed via an inherent risk questionnaire that produces an inherent risk rating that covers different security domains. Depending on the supplier's risk rating, the rating drives the assessment performed on that supplier. BMS performs pre contract due diligence based on individual risk categories. For certain third parties, background checks are done by ethics. Standard contract templates have requirements for mentioned areas. In addition, BMS also performs both cybersecurity and physical security on periodic basis. The TPRM framework has comprehensive termination and offboarding process with termination checklist that includes the return of BMS data, access, terminating access to systems or facilities. The IT team then confirms access has been revoked from users
Potection 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 5

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).

Background

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 of 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, or (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 5 of the Restated BCRs shall 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 paragraph 6.5 of the Restated BCRs shall 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 _____

THAILAND

Bristol-Myers Squibb Pharma (Thailand) Limited
Company Stamp:
Name:
Function:

Signature _____

Date _____

SINGAPORE

Bristol-Myers Squibb (Singapore) Pte. Limited
Company Stamp:
Name:
Function:

Signature _____

Date _____

EXHIBIT
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).

Background

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 of 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 paragraph 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 Business Services India Private Limited

Company Stamp:
Name:
Function:

Signature _____

Date _____

EXHIBIT
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).

Background

C. 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.

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

The parties agree:

7 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 of 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.

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

9 The BCR Adoption Agreement remains in full force and effect.

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

11 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.

12 The provisions of paragraph 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 _____

Bristol-Myers Squibb Pharmaceuticals International Holdings Netherlands B.V.

Company Stamp:
Name:
Function:

Signature _____

Date _____

APPENDIX 6

LIST OF BMS ENTITIES BOUND BY THE BCRs
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** 185 Chaussée de la Hulpe, 1170 Brussels, Belgium **Bristol-Myers Squibb Belgium S.A.** 185 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

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
SINGAPORE	**Bristol-Myers Squibb Singapore Pte Ltd** 24 Raffles Place, #15-00 Clifford Centre, 048621 Singapore
THAILAND	**Bristol-Myers Squibb Pharma (Thailand) Limited** 388 Exchange Tower, 17th Floor, Sukhumvit Road, Klongtoey,Bangkok10110, Thailand
UNITED STATES OF AMERICA	**Bristol-Myers Squibb Company** Route 206 & Province Line Road, Princeton, New Jersey 08543 United States of America