BINDING CORPORATE RULES POLICY DOCUMENT

At Bristol Myers Squibb (BMS), your privacy matters to us. For us, data privacy goes beyond mere compliance with the law. BMS aims to collect, use, and share information that we obtain about you in a manner consistent with our company values, including high ethical standards, integrity, inclusion, fairness, and transparency.

If you have any questions about the content of this document or you would like more information, please email the BMS data protection team.

1. WHAT THIS DOCUMENT IS ABOUT

This document explains what Binding Corporate Rules (BCRs) are and how they apply to personal data that BMS processes and transfers outside of the European Union (EU). In short, BCRs are BMS's publicly declared commitment to ensuring that any personal data exported outside of the EU to other companies within the BMS group are afforded the same degree of protection as offered by EU Data Protection law. BMS EU BCRs are approved by the Data Protection Commission (Ireland) through their comprehensive application process and the approved Bristol Myers Squibb Binding Corporate Rules (EU BCRs) official document (our "Legally Binding Instrument" is available here.

This Binding Corporate Rules Policy document is designed to give EU data subjects a clear, concise explanation of how BMS stands over our commitments and what rights are available to data subjects as provided by EU law - our official Binding Corporate Rules 'Binding Instrument' is available here. This document complements our Privacy Notices (available here) that provide detailed information on how we process personal data at BMS, our sources of information, how we apply EU Data Protection Laws (including the EU GDPR) to our processing of your data, and your rights as a EU data subject and how those rights can be exercised.

2. WHAT ARE BINDING CORPORATE RULES (BCRs)?

Binding Corporate Rules are a set of internal data protection rules and processes, approved by the Data Protection Commission (Ireland), that organisations must commit to when exporting personal data to another part of the same company from the European Union. BCRs are needed because some countries do not have the same high levels of data protection in place in the EU. As a multinational company operating worldwide, BMS transfers data within the BMS group of companies to fulfil a range of data processing functions described later in this document. BCRs ensure that your EU data protection law rights 'travel with your personal data' wherever the data moves within our company. For example, BMS transfers BMS EU employee personal data to our central HR department in the United States of America (USA) for the processing of employee pay and bonuses; the USA does not provide the same level of protection offered under EU data

protection law, so we commit to extending your EU data protection rights where we process your personal data in the USA.

3. WHY WE TRANSFER DATA AND WHERE TO

Bristol Myers Squibb (BMS) has many affiliates located outside of the European Union and for certain business functions we transfer data to our centralised areas of excellence located at these affiliates. As many of our centralised functions are based in the USA, BMS transfers EU data subject personal data using these Binding Corporate Rules to provide the same level of protection as in the EU. BMS has completed detailed Transfer Impact Assessments (TIA) for all our personal data transfers outside of the EU to perform a legal analysis of the legal framework of the third country importing the data. The TIA focuses on the specific transfer type: the reason and details for the transfer, the origin and destination, parties involved, the associated potential risks and mitigations in place such as technical controls, organizational controls, contractual measures and processor controls.

BMS categories it's personal data processing into the following categories:

Category	**Description**	**Country Transferred to**
Medical Marketing	Promoting BMS brands and products through marketing and advertising. This involves the transfer of: • Health Care Professional (HCP) personal data • Key Opinion Leaders • Regulatory officials and patient data.	**USA** – BMS coordinates the promotion and marketing of our products from our US offices.
Corporate Affairs and Market Access	Engaging with professional contacts, regulatory bodies, and media to expand patient access, address barriers to BMS medicine and establishing relationships with patient organizations, including grants to patient organization. This means transferring personal data of: • Health Care Professional (HCP) • Key Opinion Leaders • Regulatory officials and patient data • Members of the Public (Patient organizations representatives, members of the parliament).	**USA**– Patient access/market access programs require centralised program management in order to communicate with the country level, EU level and US authorities.
Clinical Operations	**Clinical Trials** - Monitoring data from clinical trials and management of the clinical trial to ensure that the study is being conducted to ICH GCP (Good Clinical Practice). This means transferring personal data of (key coded where required): • Patients (Participants in clinical trials, observational studies and any other clinical research); Informed consent	**USA, India–** BMS coordinates its clinical trials for specific medicines from our EU and US offices.

	• Others (Clinical Research Organization) Employees • Contractors, consultants, and temporary workers • Relations of employees • Applicants • HCPs • Patients • Business Partners • Shareholders • Key Opinion Leaders • Regulatory Officials **Site Selection** - Assessing whether a given study can be conducted on a particular site, evaluating availability of patient population and experience of study staff including: • Vendors • Pharmacy Team • investigators to conduct the study. • Data Patients (potential participants in clinical trials) • HCPs • Others (CRO team)	
Drug Safety and Risk Management	BMS has a legal and ethical requirement to make sure our medicines are used safely, record adverse event information, for specific medicines that require a risk management program, and programs to ensure patients without the financial means have access to our products. All of these programs require the processing of patient and HCP personal data.	**USA** – these programs are managed and controlled locally in the EU, but the supporting systems may be located or accessed by BMS employees from the USA and the EU.
Medical Activities	BMS provides medical information to requestors about the drug products manufactured by BMS in compliance with legal and regulatory requirements. BMS also provides our medicines under our Compassionate Use Programs. This means transferring personal data of: • Patients • HCPs • Members of the Public • Others (Caregivers and relations of patients) • Business Partners (Logistics Service Providers)	**USA** – In order to manage this activity BMS operates a centralised call centre and other teams that help manage medical requests. For our Compassionate Use Programs, although implemented locally overall program management and supporting systems is located in the USA.
Distribution/Logistics	Handling orders for BMS drugs to ensure all relevant information is contained in the Order Forms and arranging the logistics and delivery of the drug. This means transferring personal data of: • Patients • HCPs	**USA** – BMS manufactures its medicines in the USA and EU and personal data must be transferred and accessed from outside the EU.

	• Business Partners (Logistics Service Providers)	
Finance	Managing financial operations, such as account receivables, account payables, including management accounting and labour costs, and payments to suppliers, providers, grants, and donations. Also managing travel and other expenses incurred by employees to be reimbursed by BMS. Personal data transferred includes: • Patients • HCPs • Business Partners (representatives of Logistics Service Providers and other suppliers) • Employees • Others (representatives of patient organizations)	**USA** – BMS uses global systems to manage these activities and access is needed by our centre of excellence teams in the USA and the EU.
Human resources	BMS needs to process personal data for employees to provide: • Payroll • Training • General HR activities • Performance management • Employee Investigations Talent acquisition (hiring candidates) will involve the processing of: • Applicants • Contractors, consultants and temporary workers • Employees • Relations of Employees (family members for roles requiring relocation)	**USA** and **Australia**– Several HR functions are managed through global systems that are hosted in the EU, USA, UK and Australia.
Facilities	Control and managing access to BMS premises in Chester, Moreton and Uxbridge offices, including carpark and facilities – personal data processed: • Employees • Contractors, consultants and temporary workers • Members of the Public • Business Partners • Others (visitors to BMS premises)	**USA**– BMS has deployed an access management solution for our offices worldwide that is administered from the USA.

4. BMS DATA PROTECTION PRINCIPLES

The EU GDPR and related national data protection legislation is based on data protection principles that underpin our Binding Corporate Rules commitments. This means that any BMS company that has signed the BCRs is also legally bound to implementing and monitoring these data protection principles.

Legal basis for Processing Personal Data and Sensitive Data

BMS will only process Personal Data as allowed under the legal bases (Article 6) set out in the EU GDPR. These are:

- **Legitimate Interest** –BMS Legitimate Interests means the interests of our company in conducting and managing our business to enable us to develop and produce the best medicines for our patients.
- **Consent** – This means the data subject has given their permission for BMS to process their data for a specific purpose.
- **Contract** – BMS needs to process personal data to facilitate the creation and performance of a contract.
- **Legal Obligation** – BMS needs to abide by a legal requirement that requires BMS to process personal data for that reason.
- **Vital Interests** – BMS needs to process personal data when the life, health or safety needs to be protected.
- **Public Task** – This legal basis means that processing of personal data is needed for a task 'carried out in the public interest' or then an official authority order BMS to perform a specific task. For example, preventing fraud, racial and ethnic diversity within senior levels at BMS, and so on.

Special Category Data

This is personal data that needs more protection that other personal data because of its sensitivity, for example patient health data, religious beliefs and so. For more information, please see the Data Protection Commission website for more information. When we process this type of sensitive personal data, we rely on one of the legal bases mentioned above **and** where we meet one of the conditions in Article 9[1].

Purpose limitation and Proportionality

BMS collects and processes personal data that is needed for specified, explicit and legitimate purposes (as outlined in the previous section) as permitted by the EU Data Protection Laws – in other words, we tell you

[1] Article 9 Conditions:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

when we collect your data what we will use it for – we do not use it for any other purposes unless they are compatible with the original purposes.

Data minimization and storage limitation

BMS only collects and processes personal data that is adequate, relevant, and necessary for the purposes for which we collected it, and we do not retain it for longer than necessary for those purposes. In other words, we only process data that we need and no more. If the data is no longer needed, we will remove the data according to the BMS Record Retention Schedule. There may be legal reasons for us to retain the data for a specific period of time, but when this time ends, we will delete the data from our systems.

Transparency

BMS strives to be as upfront and transparent as possible when explaining to EU Data Subjects about how and why we collect and process data. Clear explanations on how EU data subject data is processed is provided at the point of collection but is also laid out in our comprehensive online notices available here.

Data quality and Accuracy

BMS places a huge emphasis on the quality and accuracy of the data we collect and process. BMS has implemented a strong Data Quality and Control process that covers all processing of personal data at BMS, with specific attention placed on our patient (and special category data), HCP and employee personal data.

Automated individual decisions

BMS does not make decisions based solely on automated processing (including profiling) of individual data unless we inform you otherwise before the processing has started. Every EU Data Subject has the right *not to be subject* to a decision that is based solely on automated processing (with no human intervention).

Security and confidentiality

As outlined in our Binding Instrument document,[2] BMS has implemented a series of Technical and Organizational Security Measures appropriate to the type of data we process and how we process that data. This includes a comprehensive Breach Management process for monitoring and responding to data protection incidents – this process covers all affiliates that are signatories to our BCRs. The clear rules set out by the Data Protection Commission in relation to the management and reporting of such incidents will apply to all EU data subject data regardless of where it is processed within our affiliates.

Data protection by design and by default

BMS has implemented appropriate technical and organisational measures which are designed to meet the principles of data protection by design and by default, as set out in the EU GDPR, and to facilitate compliance with the requirements set out in this Binding Corporate Rules Policy. Going forward, when BMS wishes to start

[2] Please see Section 4.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

new processing, it will implement any additional measures relevant to that processing to meet these principles and requirements.

International transfers to other companies

BMS will not make transfers of personal data subject to the BCRs to any company outside the EU that **is not a signatory to the BCRs** unless permitted to do so by law. This might be the case, for example, where the Government has determined that the country in which the third party is located provides an adequate level of protection, where BMS puts appropriate safeguards in place (e.g., by executing appropriate contractual clauses), or where otherwise permitted by EU Data Protection laws (e.g., where data subject has explicitly consented to the proposed transfer, where the transfer is necessary for the performance of a contract between the data subject and the controller, or where it is transfer is necessary for the establishment, exercise, or defence of legal claims.)

Accountability

Accountability in data protection law means BMS being able to demonstrate that we can comply with the law and principles set out in the previous section. All BMS group companies that have signed the BCRs are responsible for being compliant and the ability to demonstrate that compliance. For example, if data is transferred from the EU to the USA based on consent, the entity involved needs to prove that the data subject has consented to that transfer. Therefore, all entities bound by our BCRs maintains a record of all processing activities including the following information (as a minimum):

- the identity and the contact details of the controller[3]
- the purposes of the processing activity
- the categories of Data Subjects and personal data being processed
- the categories and locations of importers receiving EU personal data
- and where possible, the proposed 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.

5. YOUR RIGHTS

Every data subject can contact BMS and exercise their rights under EU data protection law. You have the right to:

- **receive a copy** of your Personal Data we hold about you
- **correct** your Personal Data we hold about you
- where applicable, **receive a machine-readable copy** of your Personal Data (portability)

[3] The data controller determines the purposes for which and how personal data is processed.

- ask us to **delete** your Personal Data or **restrict** how it is used
- where applicable, **object** to Processing of your Personal Data for certain purposes, such as when we use it for marketing purposes (opt-out)
- where you have provided us with your **consent** to use your Personal Data, you can withdraw your consent at any time without affecting BMS' use of such information before your withdrawal of consent

6. BMS Complaint Mechanism

BMS has a complaint handing process that any data subject can use if they feel that BMS is not complying by their BCRs. BMS processesa complaints according to a four-stage approach:

1. DAY 1- 4 Receive Stage
    a. BMS receives a complaint
    b. Enters the details into the Data Protection Management System
    c. Identifies the complainant and if necessary, verifies the identity.
2. Day 5-6 Acknowledge
    a. BMS Complaints Team summarises the complaint for moving to next stage
    b. Assesses if there are historical information that might be applicable to the complaint
3. Day 7-12 Analyse
    a. If the complaint can be replied to, this will happen once a Decision Review has taken place with the Data Protection Officer, Legal and relevant Business Unit Leader
    b. The team will communicate to the complainant with the BMS decision
    c. If the complainant is not satisfied with the BMS response, the move to Stage 4
4. Day 12 – 25 Stage 4 Act
    a. Escalated complaint will be sent to BMS Leadership for review
    b. In conjunction with General Counsel, BMS will reply with a Final Decision, including details on how the complainant can contact their Supervisory Authority (ICO).

Legal Redress and Compensation

All data subjects also have the right to judicial redress, obtain remedies and where appropriate, compensation for damage suffered because of Bristol Myers Squibb breaching the Binding Corporate Rules articles[4] as

[4] Data Subjects will be entitled to redress for the following UK GDPR articles and not articles related to internal processes such as training our audit process, how we update our BCRs with ICO and so on:

outlined in the BMS Binding Agreement. Irrespective of which non-EU entity breached the Binding Corporate Rules, data subjects can enforce these rights against Bristol-Myers Squibb Pharmaceuticals Unlimited (Ireland), which takes responsibility of behalf of all the BMS affiliates bound to our BCRs and will pay compensation for damages (material and non-material) resulting from a breach of these BCR articles if it is shown that one of those affiliates are at fault.

You can exercise the rights listed above at any time by emailing BMS at eudpo@bms.com or by post at:

C/O Data Protection Officer,

Bristol-Myers Squibb Pharmaceuticals Unlimited

Cruiserath Road,

Mulhuddart,

Dublin, 15,

Ireland.

Please see the BMS Ireland website for more details.

if you feel that we have been unable to resolve your information rights concern, you have the right to raise the matter with the Data Protection Commission by visiting their website or calling their helpline on +353 01 7650100.

Articles 1, 2, 3, 4, 5, 6; Article 7; Articles 8; Article 9; Article 10, 11 and 12; Article 16; Article 21; Article 18; Article 19.