




BMS GLOBAL EMPLOYEE PRIVACY NOTICE

This employee privacy notice explains you how Bristol Myers Squibb handles your personal data if you are or were part of our workforce.



WHAT YOU WILL LEARN IN THIS NOTICE

Click on the icons or text below to find out more about how, why, and where BMS uses your data:

	Who is the Controller		The type of data we process		How BMS protects your data
	Legal reasons for using your data		Why we process your data		How we obtain your data
	How long we keep your data		Who do we share your data with		Your privacy rights

- If you are a job applicant, please see here for more information: <https://www.bms.com/au/privacy-policy.html#job>.
- For specific questions about this notice or for more information on how BMS processes your personal data, please refer to the [contact section below](#).
- The online version is accessible [here](https://www.bms.com/au/privacy-policy.html#employees) (https://www.bms.com/au/privacy-policy.html#employees).

1. INTRODUCTION – HOW TO READ THIS NOTICE



In this notice, we provide you with an overview of how and why we collect your personal data – also known as personal information. We also inform you about your privacy rights related to our use of your data. You should read this notice in combination with the BMS [General Privacy Notice](#) that explains the collective privacy standards and commitments that apply to all processing of personal data at BMS. It is available on the footer of our corporate www.bms.com websites for markets where we have a presence or operate.

You can read more below about who this notice applies to and our other notices:

Before you start reading this Notice

Who is the audience?	<p>This notice applies to you during your employment and after its termination:</p> <ul style="list-style-type: none">• as a new hire, a current or past worker, including an employee and a retiree;• as a contractor, such as if you are an intern, consultant, autonomous or agency worker or a consultant;• as a third party whose information is provided to us in connection with the employment or work relationship (for example referees, family member, relative or emergency contact information).
-----------------------------	---

Country-specific notices	<p>As a supplement to this notice, there may be country specific BMS documentation covering individual country laws or processes that might impact the use of your personal data at your specific work location. These documents can be accessed through your local intranet or local HR contact.</p>
---------------------------------	---

Relevance of my personal data	<p>The nature and the categories of the personal data that BMS processes about you can differ, depending on your role and your relationship with BMS. We try to point out these differences where possible but if there are processing activities specific to your role at BMS or to the country where you reside, we will provide you with additional 'point in time information' wherever possible.</p>
--------------------------------------	---

Example: Most processing activities related to BMS employee benefits are not applicable to consultants, contractors, interns, agency workers or autonomous workers who are employed by third parties and then contracted by BMS. This notice covers personal data that BMS *controls and processes*. Contractors and consultants should therefore review privacy notices provided by their own employers to understand how their data is processed.

2. WHO IS THE CONTROLLER OF YOUR DATA



A controller decides why and how to process your personal data. However, central teams at BMS located in another country (for example, teams in the US and support services provided by our authorized business partners) may also access and process your personal data as described in this notice. For each activity, Bristol Myers Squibb Company and its affiliates will act as controller together or jointly for using your data.










Note: If you have an employment contract, the BMS legal entity who is your employer, or who has the contract with your employer, is the controller of your personal data. If you are a consultant, contractor, intern or independent worker), then the entity listed in your employer's contract with BMS is the controller.

3. CATEGORIES – WHAT TYPE OF DATA BMS PROCESSES ABOUT YOU



This section describes the type of personal data and sensitive data we collect for our processing activities, which may vary depending on your role at BMS. We describe this personal data as “**Work-Related Data**” that BMS needs for the creation of your work contracts and to run our day-to-day work activities. Remember, depending on where you live, the relevant data protection law in your jurisdiction may define personal data differently from the descriptions used in this notice.

We use the categories of personal data in the following context:

	Onboarding & HR day-to-day		Compensation, benefits & performance		Security, IT, devices & training
	Surveys, events, images, videos		Sensitive data		Environmental, health & safety
	Legal & compliance		Family data		Roles & positions, relocation, leaving

Note: Most data we use about you is necessary for our day-to-day operations. In certain cases, you might decide to participate in activities that are not mandatory, such as attending events, accessing benefits, apply to internal jobs, responding to surveys or sharing your image or video recordings with BMS. In this case, we will let you know what your options are before processing your data.

You can learn more about our purposes and why we use your data in [section 4](#).

When collecting and using your data as a BMS worker, most categories detailed below are relevant to you if you are an employee. If you don't have a contract with us but provide services to us, the categories below will not be relevant to you, for example if you are hired by a third party agency, if you are a consultant or an independent worker.

Categories of Work-Related Data

Most of the personal data collected at BMS is done during the onboarding phase. The data collected during this stage allows BMS to build your profile and enables you to work at BMS. Examples of data collected are:

Onboarding data

- CV, past experiences, external affiliations;
- BMS ID, login details, professional phone number;
- current and past roles within the organization;
- your hiring manager, HR business partner, department, functions;
- employment contract and current employment situation (temporary,

permanent, practice), group and projects you belong to;

- initial and termination date, offer of employment, contractual conditions, signature, salary grade and bonus, promotions.

You can read more information about the data we collected during your recruitment to BMS in our [General Privacy Notice](#).

Your contact and ID information includes your:

**Contact and
identification
data**

- full name, title, location;
 - postal code and/or personal email address, personal and professional phone numbers;
 - date of birth;
 - gender, nationality, photo;
 - government-issued identification (national ID, driving license, passport, professional license number as applicable);
 - unique personal identifiers, such as your assigned unique BMS ID.
-

Data related to your previous or current role(s) at BMS, such as:

Employment data

- previous or internal applications;
 - resignation, termination dates;
 - your resume or CV;
 - office address, department;
 - performance and disciplinary records;
 - academic/professional qualifications;
 - immigration status and documentation;
 - residency permits and visas, occupational health assessments, work-related accidents, training data;
 - occupational health assessments and work-related accidents, training information.
-

**Educational and
professional data**

- education information and professional qualifications;
 - professional networks;
 - training records;
 - employment status;
 - skills and work experience;
 - programs, such as training, certifications, coaching, driving improvements if your role requires to drive a vehicle (i.e.: logistics, customer visits);
 - publications and activities;
 - awards and recognitions;
 - teaching posts, board memberships, membership or directorship in various professional organizations, associations or other units, referrals and other relevant professional information where needed.
-

Family & data of your relatives and third parties	<p>You may share contact details of family or relatives in case of relocation, services, accidents, or emergency situations, such as:</p> <ul style="list-style-type: none"> • family or your relatives' contact data, including e-mail, personal phone number, home address; • full name and specific needs for residence of partners and family members.
Conflict of interest data	<p>BMS may also request to inform us about your potential conflict of interests which can include:</p> <ul style="list-style-type: none"> • contact details, positions of third parties with whom you belong or have professional interactions with; • shares, stocks, participations in or partnerships with non-BMS affiliated organizations, including serving as director or officer of such organization; • any potential gifts, financial interest or advantage, honorarium or other remuneration you may receive outside of BMS.
Sign-in, analytics and device data	<p>When using BMS or third-party devices, platforms, intranet, systems and technologies, we use your personal data to provide you access to, tailor the services provided to, and to protect the security of, our systems. We use the following types of data:</p> <ul style="list-style-type: none"> • sign-in and log activity data; • device ID and IP address, usage data; • information accessible in your profile; • abnormal use of devices warnings, for BMS platforms, intranet and systems for security and protection of BMS assets; • application or interaction data in BMS or third-party platforms; • personal data stored on BMS devices, platforms, intranet and systems, such as documents you upload and your emails. <p>You can read more information about the use of your personal data or digitally in section 5 below.</p>
Financial information, compensation and benefits	<p>We collect financial information about you for pay-roll, benefit, and insurance purposes, which can include your:</p> <ul style="list-style-type: none"> • bank and account details; • salary and compensation data; • travel and expenses for work, authorized trips for reimbursement purposes; • stock options, stocks, company shares; • pension fund related data; • health plans, benefits, insurance allocations; • severance package or benefits that apply when your employment with BMS comes to an end.

<p>Data about you that we make public</p>	<p>There are instances when you agree or where we must disclose your personal information publicly on our corporate websites, public registries or public facing platforms – this will depend on your participation at BMS events, posts on social media, and your position and role at BMS.</p> <p>For example, your:</p> <ul style="list-style-type: none"> • full name, e–mail address; • position within BMS, CV, professional background; • compensation and benefits; • position on a board of directors; • photos, audio, or video recordings; • quotes and posts on social media about corporate news, scientific research, events.
<p>Other data</p>	<p>Tax status, information related to work attendance, travel and expenses, emergency contact details, compensation, hours of work, holidays and benefits related information, CCTV data and investigation related information.</p>
<p>BMS often collects personal data that can be considered as sensitive in your country where you work. Read more details below about what categories of sensitive data BMS may collect and use about you:</p>	
<p>Sensitive Work–Related Data</p>	
<p>Health, welfare and leave information</p>	<p>This information if needed for managing your leave and compensation:</p> <ul style="list-style-type: none"> • number of sick days; • doctor’s certificate / medical certificate for sick leave, short–term and long–term disability, medical accommodations; • any known disability / workplace accessibility needs, for purposes of salary payment, workforce planning, and compliance with legal obligations; • work–related accident information, compensation, work safety and compliance with legal obligations (such as reporting obligations); • personal health status for commercial insurance or participation in various activities for example if you participate in sport activities, health programs or for support of your illness.
<p>Vaccination or health status</p>	<p>On certain occasions, where applicable and permitted by applicable law, in particular for public health or protection against diseases (i.e.: pandemic situations) BMS may collect your health status, such as:</p> <ul style="list-style-type: none"> • presence at work or at home; • vaccination, health status. <p>In most cases, BMS will collect your data indirectly, without the need to obtain</p>

	health information, to protect against the spread of infectious diseases or to ensure a safe working environment.
Background check data	<p>This includes if relevant to your role and permitted by local law:</p> <ul style="list-style-type: none"> • background checks or criminal records, (e.g.: in the context of fraud or crime prevention in the logistics, packing and shipment using airlines). • creditworthy information; • document certification authenticity; • personal or professional references and recommendations by previous employers or third parties;
Religious beliefs	<p>This can be collected or required by applicable law:</p> <ul style="list-style-type: none"> • for tax declaration purposes; • as written in your ID card or passport; • for internal purposes, if you share this information voluntarily.
Race and ethnicity data	<p>We will usually only collect and store such sensitive data anonymously for equal opportunities monitoring purposes or if you decide to share it for a defined purpose. Only where permitted or required by applicable law and where relevant to your role.</p>
Trade-union / labor-union membership	<p>If applicable in your country, BMS or competent authorities may request you to provide your professional contact, membership of affiliation to works councils, trade-union details, or other employee representative bodies.</p>
Sexual orientation data	<p>Where required or permitted by applicable laws or you have voluntarily provided the information to us. For example:</p> <ul style="list-style-type: none"> • marriage, maternity, paternity, parental, bereavement, other similar leaves relating to family or your personal situation; • marital status, family, relatives contact information. <p>Most often this data will be stored anonymously unless you decide to share it for another defined purpose.</p>
Other sensitive Work-Related Data	<p>Depending on the law of your country, BMS collects other categories of personal data about you that can be considered sensitive, such as:</p> <ul style="list-style-type: none"> • your health information if you participate in pilot/test programs in the context of digital health initiatives; • bank details, social security number, driver's license number, email content and text messages, State ID card number, passport number, creditworthy information, precise geolocation data; • dietary restrictions, health conditions; • on rare occasions, genetic, biological data in the context of laboratory tests to protect your health if you are exposed to biomaterials, chemical

compounds;

- biometric data, such as your fingerprint data to enter our premises, facilities.

Only authorized teams and approved third parties will have access to your sensitive personal data.

4. PURPOSES – WHY WE PROCESS YOUR DATA AND IN WHAT CONTEXT

This section describes the main types of activities where BMS processes your personal data and the context in which BMS uses it. Our main processing activities consist of:



- **handling your data for day-to-day operations**, such as for onboarding you as a new hire or worker, handling your payroll, requests, enabling access to our systems and intranet and BMS social media platforms to interact with other colleagues, for internal interactions, and if applicable performance reviews;
- **offering benefits**, such as learning, career development programs, fitness, rebates on goods, well-being programs, BMS or external events/initiatives;
- **implementing appropriate security measures** and infrastructures that prevent data losses, ensure compliance with applicable laws, maintain whistleblowing hotlines and channels to report misconducts, conflict of interest or unlawful behaviors which may require preserving information as evidence to comply with applicable employment legislation;
- **in the context of our working culture** and environment as multinational company, such as participating in diversity and inclusion groups, activities or discussions, responding to surveys about the working environment at BMS.

You can read more details about the context in which we use your data below.

Category of data	The purpose for use
Relocation, local assignments of workers	BMS processes your data for the following reasons: <ul style="list-style-type: none">• managing your relocation to other locations;• to apply for a working visa or residence permit;• for employment related information to comply with applicable laws, such as tax filing purposes, passport or other citizenship and right to work documentation, information collected for visa and immigration purposes;• family related data for insurance, travel, costs and expense purposes.

Onboarding and administration	<p>When joining BMS as a new hire, to:</p> <ul style="list-style-type: none"> • register your emergency contacts and emergency notifications in the event of business continuity response measures or for workspace security; • determine incentive and corporate credit card eligibility; • establish worker location, to manage internal transfers within BMS and off–boarding/termination, for business travel purposes; • manage the workflow, such as assigning, managing, administering projects; • enable organizational development, preparation, management, and use of an internal business directory, organization charts; • record trade union membership where required by local law.
Talent acquisition and recruitment	<p>After your application has succeeded, BMS uses your personal data to further process your job application, record your information in our systems, at a later stage for any internal job opportunities, projects or initiatives that might be applicable to you and your career at BMS.</p>
Attendance administration	<p>In some cases, BMS may record your on–site attendance in the workplace in compliance with internal policies and as permitted by local law.</p> <p>This includes data necessary to record and administer your working hours, attendance and overtime application, approval and reimbursement when applicable or compliance with the applicable BMS flexible way of working policy.</p>
Leave management	<p>To enable your leave application for paid annual leave and unpaid leave:</p> <ul style="list-style-type: none"> • health and medical data, such as the number of sick days; • doctor’s certificate/medical certificate; • information on work–related accidents; • insurance claims; • information on disability; • information on marriage, maternity and parental, military or civil service assignments, or bereavement leaves.
Compensation and benefits	<p>To comply with legal requirements and BMS labor policies related to compensation and benefits, which includes:</p> <ul style="list-style-type: none"> • offering of social security insurance, pension, housing fund and other flexible benefit programs and wellness initiatives, such as commercial medical insurance, annual medical examination, other allowances, based on your jurisdiction; • offering well–being services, rebates, points for goods and services, car fleet services; • administering employee welfare activities that participants may voluntarily participate in (including welfare provided for former employees), such as team–building activities, recreative and event activities including with your family, labor union activities, and aid

	service, where applicable.
Learning and development	To manage talent development, administer and track training and awareness activities.
Performance and recognition	<p>We use your performance data to:</p> <ul style="list-style-type: none"> • enhance performance evaluation, promote personnel development, improve worker efficiency; • set performance objectives, evaluate performance; • provide you with recognition and awards, to manage promotions.
Working culture and BMS events, surveys and activities	<ul style="list-style-type: none"> • to improve the working culture at BMS, provide you with a friendly working environment; • to conduct surveys, hold events and other activities that you could participate in voluntarily.
Travel and expense reimbursement	<ul style="list-style-type: none"> • to book travel and accommodation; • to review and evaluate reimbursement applications, record the supporting documents including transaction records for business expenses; • to make reimbursement payment to an employee's bank account; • to ensure compliance with travel & business expenses policies.
Safe work environment, information security, acceptable usage, fraud detection and prevention	<p>The nature of the work at BMS requires us to protect the health & safety of its employees, data, and infrastructure. BMS processes your data to:</p> <ul style="list-style-type: none"> • ensure security and systems monitoring (for example through video (CCTV) recording); • ensure the security and integrity of BMS facilities, IT systems and data; • notify you by phone or electronic notifications about events or incidents happening while you are traveling for work; • administer, monitor and/or manage appropriate usage of BMS premises, property, and equipment, such as requirements of identity verification and access control to device, hardware, software, internet, network, infrastructure, cell phone, mail service, or other facilities.
Protecting health & safety of its workers or third parties	<p>BMS internal policies to protect against serious diseases or threats in the context of:</p> <ul style="list-style-type: none"> • exposure to chemical or biological compounds in our manufacturing sites. • global, regional, or national public health, for instances in the event of pandemic situations. <p>In such cases, BMS may collect, or require third parties to collect, information that demonstrates your health or vaccination status.</p>

<p>Compliance and regulatory purposes</p>	<ul style="list-style-type: none"> • to ensure corporate compliance requirements and policies are met, including conflict of interest declaration and review, audit, completion of mandatory training, prevention of cybersecurity incidents; • to manage, review and respond to complaints, investigations, and disciplinary matters, to establish, exercise or defend legal claims or other legal rights; • to monitor and track of the different cases and their resolution, and definition of the nature or cause of the investigation; • to comply with applicable laws (such as tax deductions and declarations), regulations and requests from governmental agencies, and to adhere to industry standards.
<p>Equal opportunity and diversity monitoring / initiatives</p>	<p>When using this data in limited, permitted or required cases, we may collect:</p> <ul style="list-style-type: none"> • race, gender, ethnicity, veterans and disability data, such as information contained in your passport or other citizenship documentation and right to work documentation or information collected for visa and immigration purposes or to comply with local government regulations. • sexual orientation, diversity data where this has been provided voluntarily to BMS.
<p>Understanding the diversity of our workforce</p>	<p>We collect certain demographic data mostly in aggregate, such as:</p> <ul style="list-style-type: none"> • race, gender, ethnicity, sexual orientation, veteran and disability status to help us understand the diversity of our workforce and to support core business diversity, equity, and inclusion initiatives. • in some circumstances, we may also need to use this data to comply with government regulations. <p>Note: we generally collect this information on an aggregate or on a voluntary basis, and you are not required to provide it unless it is necessary for us to comply with a legal obligation. We will not share your data without your permission unless we are legally required to do so.</p>
<p>Run security & compliance scans or verifications</p>	<p>In certain countries, BMS will monitor your individual activity only if we have a reasonable, proportionate, and robust legal reason in place. Typical examples of where BMS might monitor your activity are:</p> <ul style="list-style-type: none"> • your physical movement using CCTV, badge data or sign-in sheets – this is for the security of our employees, visitors and BMS property. • your interactions with customers (for example HCPs) – this is only conducted for specific job roles at BMS and is done for training, verification, and quality assurance reasons; • network scans including your electronic activity when using our communications systems and networks. This can cover logfiles, use of BMS assets and systems. The reason for monitoring might be network and device management, protecting our intellectual property (IP), protection against cyber-attacks, certain legal

obligations, but always where permitted by law;

- for specific investigations, for example if an employee is strongly suspected of breaching BMS policies.

This type of monitoring will always fully comply with the law and will only process the least amount of data needed to complete the investigation.

Automated decision making

In general, BMS does not make employment decisions based solely on automated processing (including profiling) of employees. If this were to happen, for example using Artificial Intelligence, then BMS will make you aware of this activity before any of your personal data is processed.

You can learn more about the technologies we use in [section 9](#).

Criminal records and background checks and verification

BMS run background verifications to confirm the accuracy of documentation you provide to BMS during and after your hiring process, but only where permitted by the law and where relevant to your role.

Examples: criminal records, education, employment verification, creditworthiness, conflict of interests checks.

Other processing activities

BMS may require you to provide certain personal data (such as your name, address, and ID number) of other individuals (for example, family members) for other purposes such as:

- managing your employment relationship with us;
 - contacting you or your personal contacts during emergency;
 - declaring a conflict of interest;
 - filing tax returns;
 - processing any corporate group insurance plans;
 - participate in BMS activities or enjoy benefits provided by BMS.
-

Note: As a BMS Worker, you are responsible for any sharing with BMS of personal data about persons outside BMS – for example, providing BMS with information about family members for health insurance purposes, relocation services, conflict of interests, verification to past employers, emergency contacts and so on. Therefore, it is your responsibility to inform the third party about such disclosure or where required, obtain their prior permission, and provide them a copy of this privacy notice.

When disclosing the personal data of these individuals, you will be acting on their behalf.

5. ENTERPRISE PLATFORMS & DEVICES – HOW WE USE YOUR DATA

As a BMS Worker, there are many times when we need to process or share your data using digital means.

In most cases, your online connection to BMS systems is securely managed through the BMS single sign-on (SSO) process or through our VPN (virtual private network). You may access other systems, such as Outlook or Workday using double factor authentication.



For more information about how we collect personal data from visitors to our websites or users of our products and services, please review our [General Privacy Notice](#).

You can read more details about how we use your personal data through digital means below:

Type of activity	Data categories	Purpose for use
BMS intranet, websites, and applications	Login data (BMS ID, login details for SSO), Analytics data	The main use of your personal data for our intranet sites are for: <ul style="list-style-type: none"> enabling you to connect to our systems; audience measurements and aggregate websites' traffic and analytics.
Eligible programs, benefits or activities run by third parties	Eligibility contact data (BMS e-mail, BMS ID, full name, role if needed).	BMS shares your contact details with trusted third parties to offer various benefits to workers who are eligible to access such programs.
Matching your profile for internal opportunities	Application data (full name, BMS ID, your skills, interests, current role). Professional data (such as your CV/resume, data from 3 rd party platforms such as LinkedIn).	When you enter your professional data into BMS HR systems, BMS can use that data to propose internal opportunities at BMS that might be relevant to you. When doing so, BMS sometimes uses third parties to help match your profile to the most suited available job roles. When we do use external providers and/or software for this activity, you will receive more information prior to our use of such data. Read more in section 9 about Artificial Intelligence and section 10 about your privacy rights.
Bring your own device (BYOD)	Device ID and other data needed to secure the connection to BMS application and systems.	Where permitted under BMS policies, you may also use your own device (Bring Your Own Device (BYOD)) or other approved devices to perform your job at BMS. This requires BMS to access your personal data to enable your device, including the installation of BMS approved software for information protection purposes.

Cybersecurity & information protection

Aggregate security data, system monitoring data and contact details and usage data

BMS uses a variety of supporting applications and teams to ensure all data remains available, secure, and confidential when you use BMS approved, technologies and systems. To achieve this goal, BMS processes your data for the purposes of updates, diagnostics, tests, and the security of your laptop or devices.

Example: To prevent data losses, phishing or scam attempts or for compliance purposes, we may send you notifications, personalized reports or refresher training requests.

6. DATA SOURCES – HOW DO WE OBTAIN AND SHARE DATA ABOUT YOU



BMS collects personal data directly from you for most of our processing activities, although sometimes we obtain personal data automatically through certain internal BMS sites or indirectly from alternative sources.

For example: we collect personal data indirectly from service providers (such as recruitment agents and background checking services), online platforms, government bodies (criminal records, wage garnishments) or authorities where required by law (such as tax authorities) to manage your work relationship with us.

We also collect information about you automatically, through physical or online security, systems monitoring (for example through video (CCTV) recording) or building access control logs when you enter the workplace or in other similar contexts. BMS will always strive to make you aware of this type of processing before collection of your personal information takes place.

7. DATA TRANSFERS – WHO WE SHARE YOUR DATA WITH AND WHO CAN ACCESS IT



Only limited BMS teams and approved third parties or authorities who need to manage or obtain your information may access Work-Related Data. When your personal data is more sensitive, BMS will apply more restrictions and protections to protect it. For details on our cross-border transfer mechanisms, please see the relevant section in our [General Privacy Notice](#) available on all bms.com websites.

Read more about how we share your Work-Related Data and who can access it below:

Inside the BMS group

BMS locations BMS is headquartered in the **United States**, with operations in **Europe, Asia, Australia** and in **North and South America** – all collectively known as the “**BMS group**” (of companies).

Given the global nature of our company, processing of employee data occurs across several countries. Many of our HR processing activities are centralized in the United States (for example in our Tampa office), but we also have centralized HR activities in Australia, China, India and the United Kingdom. Your data will be accessed by local and central teams who may be located in such locations.

You can also find the main locations from where we operate here: <https://www.bms.com/about-us/our-company/worldwide-facilities.html>.

Contracts and principles to secure the transfer **Binding Corporate Rules** (BCRs) is a recognized mechanism that allows the transfer and disclosure of personal data across entities that are part of the same company group. Our [Binding Corporate Rules Policy](#) provide you with an overview of our global privacy program and commitment to maintaining high data protection standards when processing personal data transferred to different countries within the BMS Group of companies.

Transfers of Work-Related Data also occur based on appropriate arrangements including data transfer agreements, local or regional transfer schemes or, when appropriate or required, your consent.

Teams or function accessing your data BMS teams who can access your information include:

- **HR departments** and hiring managers in the context of the employment relationship;
- **BMS functions**, such as finance, internal audit, IT, the law department and records management in the context of their functions and responsibilities;

- **corporate directory** (BMS Whitepages): all the employees of the BMS group of companies will have access to the business contact details (name and surname, role and function, manager, email, where applicable phone numbers and business address).

Outside of the BMS group

Why we need to disclose your data BMS partners with many organizations that are specialized in areas such as IT, security, tax and accounting, payroll, providing benefits, running programs, insurance, pension, or other services. In other cases, we disclose your data to authorities.

Approved third parties BMS engages with a variety of third-party service providers to help support the services we provide to our workers. For many of our HR functions, the third-party service providers are embedded within our HR functions (for example as consultants providing IT Support services) but in other instances, you will have a direct relationship with the external vendor – for example, insurance providers, health, and wellness Apps and so on.

Governmental bodies or authorities BMS may share Work-Related Data that includes your contact details, correspondence, internal or external communications with authorities or for dispute resolution purposes, claims or investigations, to comply with applicable laws or to protect BMS' business or interests.

Security BMS puts all third-party vendors through a series of rigorous security and privacy checks, regardless of whether the vendor works directly for BMS providing a support service or whether the relationship with the vendor is directly between you and them. In addition, we have data protection clauses included in all our contracts with vendors, where needed, to ensure that the applicable data protection legislation is followed regardless of the country in which your data is processed.

8. OUR LEGAL BASES FOR PROCESSING YOUR PERSONAL DATA

In this section, we describe our legal justifications (commonly referred to as “legal basis”) for the use of your data related to each of purpose for using it. We will use the legal basis that is most appropriate for the purpose and circumstances related to such processing. Below, we have explained which legal bases we may choose or have to use when using your personal information.



Note: Depending on the country or State where you reside, the law of your country may not require that BMS justifies how it uses your data (such as in the US or Hong-Kong). This applies to ordinary use of your data, transfers outside of your residence, or when sharing or disclosing your Work-Related Data with a third party. If you are from a jurisdiction or a State that requires a legal basis for processing personal data (such as China, the EEA, UK, or Brazil), our legal basis will depend on the personal data concerned and the context in which we collect it. Where required by applicable law, BMS will obtain your prior consent for certain processing activities – for example, using cookies or trackers, when using your images or recording

materials, disclosing your personal data outside of your country of residence or disclosing it with BMS-approved third parties.

You can read more information and examples of legal bases we use to process your data.

BMS relies on a legal basis for each of our processing activities for most of the jurisdictions where BMS operates, whether relating to Work-Related Data or Sensitive Work-Related data. However, the privacy laws in some countries may not require the same legal basis for our processing activities as we have described in this notice. For instance, we may use consent or contractual necessity instead of legitimate interest when the local law does not recognize such a legal concept.

Our most used legal bases are:

- **contractual necessity:** in practice, this means that BMS needs to process your data to honor our commitments as stated in your arrangement with BMS, for example providing your personal data to our third-party payroll, pension or insurance provider;
- **compliance with a legal obligation:** there are many times where BMS has a legal obligation to use, retain or disclose your Work-Related Data. We will make this clear at the time and inform you whether provision of your personal data is mandatory or not, as well as the possible consequences if it is not provided;
- **prior consent:** where BMS conducts optional activities or when the law requires it, we will inform you and BMS may require your **prior consent**. Unless the nature of the activity or of the data requires it, your local law prescribes or allows otherwise, you will have the right to withdraw your consent at any time;
- **public disclosures:** if you agree to disclose your Work-Related Data publicly or if BMS has a duty to do so, then future control over that data may be compromised. BMS will provide you with a notice explaining the processing activity where your personal data may become publicly available and if you have a choice of whether to participate or not.

Legal basis	Description and examples when using our legal basis
Performance of a contract with you	<p>In most cases, we justify using your data for HR management as described in our HR related policies, handbooks and other rules that may apply to your role at BMS.</p> <p>Examples: Compensation & benefits, performance, ensuring compliance with employee handbooks, SOPs, internal procedures, for sick leave, internal career development and opportunities, running our daily operations, login to and use our IT systems.</p>

Legal obligations, investigations, and compliance We use your personal data when BMS complies with its **legal obligations** related to employment which can include Sensitive Work-Related Data.

Examples: in the context of tax laws, regulations preventing anti-bribery or conflict of interests, public health, for security, health & safety at work, investigations or internal or third party claims, audits, good clinical, laboratory and manufacturing practices (GxPs). This includes sharing your Work-Related Data with third parties or competent authorities or bodies.

Legitimate interest or use BMS has legitimate interests to use your personal data for identified purposes, but we will always assess that there is an appropriate balance between your right to privacy and BMS's interest to conduct its business operations.

In general, BMS considers it has a legitimate interest to use your Work-Related Data to achieve its immediate and long-term business and commercial goals and outcomes, such as in the context of:

- recruitment and candidate selection, and HR management;
- protecting our work case management, running investigations to evaluate misconducts or non-compliance with internal policies or procedures, retaining data for protecting against claims and disputes, business continuity, pension, or retirement administration;
- celebrations of special occasions (recognizing years of service, birthday), using intranets, corporate directories, make your BMS profile available internally or to our approved third parties;

-
- prevention and detection of data loss, crime, or fraud;
 - manage and forecasting our finances;
 - conduct surveys, analytics, improve facility accesses, workforce optimization, security of our systems or prevent data losses.

Note: BMS uses its legitimate interest when it is proportionate, aligned to, or does not conflict with your reasonable expectations, and does not undermine your individual rights, interests, or freedoms.

Consent In the context of voluntary initiatives or benefits that you can access where we obtain your **prior permission** to use or share your personal data for a specific activity, such as events, picture, or recordings, connecting to third party platforms or services.

Public interest To protect against serious diseases or threats in the context of global, regional, or national public health, for instances in the event of pandemic situations. In most cases, accessing or disclosing your personal data in this context will be based directly on applicable laws.

Vital interest On rare occasions, we use your vital interest to protect you or the vital interest of third parties, for accident, security or to prevent imminent threats to your or third parties' health and safety at the workplace or outside our premises for emergencies or insurance purposes.

The list above is not exhaustive and is intended to provide you with an overview of how we justify the processing of your personal data.

9. DO WE USE ARTIFICIAL INTELLIGENCE (AI) OR SIMILAR TECHNOLOGIES?



BMS has developed internal policies and guidance on responsible use of Artificial Intelligence (AI). When using AI tools involving Work and Sensitive Work-Related Data, we apply globally recognized data privacy and protection principles. When using third party technology, we apply:

- (i) BMS principles on responsible use of AI.
- (ii) Appropriate technical and security measures.
- (iii) Contractual arrangement to protect your personal data.

BMS will provide you with more detailed information in a privacy notice, and if required, obtain your prior consent before using such technologies.

You can read more information about your rights, including your right to object or to request human intervention, in [section 10](#).

Currently, BMS does not use technologies that qualify as Artificial Intelligence (AI) when worker personal data, such as algorithms that have a sufficient degree of autonomy to make important or significant decisions about you in the context of work without human oversight before any decision is made. In other words, BMS does not use such technologies without decisions being made by humans which can affect you as a BMS worker.

However, we do use certain tools and technologies that allow us to improve efficiency in our daily operations. BMS is looking at digital solutions, automation and advanced technologies that can:

- **reduce manual tasks**, to support our operations and drive efficiency at work;
- **improve your well-being**, safety at the workplace, mental health;
- **assess risk profiles** to comply with internal BMS policies and applicable laws, such for, anti-bribery, drug promotion or preventing conflict of interest;
- **protect BMS systems**, including in the context of cybersecurity or data loss prevention programs;

- **facilitate the selection of potential candidates** for recruiters' review when applying on our official careers website: <https://careers.bms.com/au/>;
- **send automated instant messages** and communications through intranet or online chatbots, calendar scheduling bots, or other online technologies. Internal chatbots may use our enterprise directory to refer our teams to the appropriate subject matter experts; and,
- **match your BMS profile** for career development opportunities.

Example: BMS may use machine learning solutions that can enable career or learning opportunities at BMS, on a voluntary basis, including to suggest internal projects, reach assignments, tour of duties or job opportunities that match your profile and to propose boosting your career at BMS.

10. INDIVIDUAL CHOICES – RIGHTS AND ACCESS TO YOUR DATA

This section describes the rights you may have and the potential actions you can take in relation to how BMS processes your personal data.



You have several privacy rights in relation to the processing of your personal data at BMS, but these will depend on the country where you reside and on the legal basis that we used to process your personal data. Exercising your rights is usually free of charge, except if your request is excessive or requires disproportionate efforts, in which case we may ask you for a reasonable fee.

BMS assesses every request received based on who you are and the jurisdiction or State in which you are based. If we cannot comply with your request, we will let you know the reasons why. You can always contact BMS at contact.australia@bms.com to find out more about your rights and how you can exercise them.

The rights described below are not absolute and will only apply in certain circumstances. This means that we may be unable (for example, due to legal requirements) or not obligated to act on your request. In some cases, we may need to collect additional personal data from you to verify your identity before we provide access or delete your information, for example a copy of your government-issued identification.

Right of access	You have the right to contact BMS and request confirmation that we process your personal data, why we process your data, and be provided with access to that data. Please remember that this is not an 'absolute right'; there are situations where we must remove or redact data to protect other data subjects and company confidentiality.
------------------------	---

Right to rectification	You may have the right to update/correct your personal data, for example if it is inaccurate, incomplete, or not up to date.
-------------------------------	--

Right to erasure (right to be forgotten)	You may have the right to have your personal data deleted. There are exceptions to this right, for example when we are legally obliged to retain your personal data for a specific time-period, or when your data is disclosed publicly.
Right to restrict the processing	You have the right to request that we restrict, suspend, or cease the processing of your personal data. Exceptions also apply here. If BMS lifts the restriction, we will inform you beforehand and explain our reasoning.
Right to data portability	You have the right to receive or have your personal data transferred to a third party in a structured, commonly used, and machine-readable format. Note: This right may not apply when your data is processed based on the legitimate interest of BMS or in certain jurisdictions.
Right to withdraw consent	When we process your personal data based on your consent, you have the right to withdraw it at any time and BMS will stop processing your personal data. However, the withdrawal of consent does not impact our processing of your personal data prior to the removal of your consent.
Right to object	You may have the right to object to BMS processing your personal data. This is also not an absolute right and your right to object will depend on the nature of the processing by BMS.
Account deletion	Where applicable, you may have the right to request to delete your user account. This applies for example when using an account on a platform that is operated by a third party. In this case, please contact the platform directly to exercise your rights.
Right to complain to data protection authorities	In some countries, you may have the right to complain directly to the data protection authority in your jurisdiction, if you believe that BMS is processing your personal data unlawfully and/or is violating your rights. The privacy rights section of our BMS General Privacy Notice describes how to contact the competent authority or relevant contact in your country where you reside.

You can read more below about the actions you can take about your personal data:

I would like to	Tools you can use to manage your data
Update my data	Workday, myBMS and e-mail. If your personal data changes during the course of your time at BMS, please raise a ticket or connect to your Workday account to update that data or contact your HR business partner to note those changes.

Access my data or receive a copy of my data **Workday, myBMS, and e-mail.** Workday and the relevant applications available in myBMS allows you to see the data that we hold about you and download a copy.

If we have data that you cannot access through Workday, then you may make a request by raising a ticket via MyBMS or using the contact details provided in the [contact us](#) section below.

Note: We might refuse access to personal data in certain cases, such as when providing access might infringe someone else's privacy rights.

Delete my data or withdraw consent

Workday, myBMS and e-mail. You can ask that we delete personal data that you believe is inaccurate or no longer relevant by raising a ticket via MyBMS or using the contact details provided in the [contact us](#) section below.

In addition, you can go into Workday and remove some of the data you have chosen to share with us, such as your photo, demographic data, emergency contacts and so on. We might need to refuse deletion of personal data in certain cases, for example if there is an impact on our legal obligations.



11. DATA SECURITY – HOW WE PROTECT YOUR PERSONAL DATA

BMS uses appropriate technical and organizational measures to protect your personal data online and offline. We do this to prevent unauthorised processing, loss of data, disclosure, use, alteration, or destruction of your personal data. The measures that we deploy are dependent on the sensitivity of the personal data and the most recent advancements made in security technology. Where appropriate, we use encryption, pseudonymisation (such as key coding), de-identification and other technologies that can assist us in securing your data, including measures to restore access to your data. We also require our service providers to comply with reasonable and recognized data privacy and security requirements.

Bristol Myers Squibb has adopted the **NIST Cybersecurity Framework** (<https://www.nist.gov/cyberframework>) to ensure that our most critical information is kept confidential, suitably available, and safeguarded from corruption. Aligning with NIST also allows us to continuously assess and improve our ability to protect, detect, and respond to cyber attacks. NIST defines five cybersecurity functions: identify, protect, detect, respond, and recover. We have aligned our cybersecurity program to these five functions.

We conduct regular testing and reviews of our technologies and processes, including auditing of our business partners and vendors, so that our security controls remain effective and up to date. Also, we may further anonymize your personal data when it is no longer needed for the purpose for which BMS originally collected it.

12. DATA RETENTION – HOW LONG BMS RETAINS YOUR PERSONAL DATA

Data retention schedules



BMS will only retain your personal data for as long as necessary for the processing purposes listed in [Section 4](#) above. When retaining and storing data about you in our systems, we have put in place specific data retention schedules in accordance with our company policy and in compliance with applicable data protection and local employment laws.

Criteria to keep your data

Typically, we retain data based on the following criteria:

- the quantity, nature, and sensitivity of the personal data in question;
- the potential risk of harm in the event of unauthorised use or disclosure;
- the purposes of the processing;
- whether or not these purposes can be achieved by other means, as well as the applicable legal obligations.

Note: the below retention schedules are not applicable across all countries – certain retention periods may differ from this table to meet local legal or regulatory requirements (such as China). Retention periods can also be adjusted in line with specific changes made through new legislation.

There are instances where BMS is legally obliged to adhere to specific retention periods. For example, when BMS must retain data for a set minimum period or to delete it after a set maximum time limit. Some common examples of these obligations normally relate to data needed for tax and accounting, anti-bribery, conflict of interest or investigation purposes.

Type of activity	Retention period
Benefit plan administration, reporting, and participant disclosure	Event + 10 years
Benefit enrolment and participation	
Benefit plan development and management	Event + 6 years
Benefit plan texts and amendments	
Education assistance, and work/life and diversity	Creation + 7 years
Workforce tracking and compliance	Creation + 5 years
Employee recruitment and selection	Creation + 3 years
Employment eligibility / verification & immigration	Duration of employment + 6 years
Personnel relations & investigations	Event + 3 years
Personnel records	Duration of employment + 7 years

Training completion – general	
Labor arbitration / grievances	Event + 50 years
Labor relations records	Creation + 50 years
Compensation / salary, and incentive planning	
Training programs and materials	Active + 5 years
Training relating to BMS products in compliance with GxPs	Active + 2 years. Thereafter, the longer of 25 years or 10 years after the expiration of the drug’s marketing authorization.
Employee relocation and forgivable loans	
Payroll	Creation + 11 years
Payroll tax records	
Employee time and attendance records	
	Creation + 8 years

For more specific information about the description of each activity, how long BMS retains your personal data for human resources management, or for other purposes as described in this privacy notice, please access this page: <https://retention.bms.com>. If your relationship with BMS does not allow you to access this page, please contact us at contact.australia@bms.com.

13. LEAVING BMS – WHAT HAPPENS TO MY DATA

After you end your employment with BMS, we retain certain information about you (for example, your contact details) to fulfil certain business operations, to administer or manage retirement plans, payment for outplacement services, or respond to queries from your new employer.

You can read more below about why we may retain your data after you leave BMS:

Purpose	Categories of data	Details
Claims & disputes, legal hold	For example, compensation, incident data, e-mail exchanges, investigation data.	To deal with claims or disputes involving you or others. This could include an accident at work. We do this because we have a legal obligation to provide the information, or it is in our interests to bring or defend a claim. We may also have an obligation to retain and preserve data or evidence that is subject to a legal hold obligation.

Retirement, e-mail communications or referrals	Years of service, compensation, e-mail exchanges, your applications and new role, third party contact details.	We may keep or share your information to administer or manage leave, severance or retirement packages, contact you in relation to your past role or work or to respond to queries to your new employer about your role at BMS.
Outplacement services	Professional and personal contact details, CV, professional background, role at BMS.	BMS may offer or pay for services after you leave our company. BMS will only keep your data necessary to pay the costs of packages you may be eligible for.
Business continuity	E-mails and documentation, projects, and decisions you made, login and accesses to systems.	To understand and evidence decision making in your role and maintain knowledge within the business after you leave. We do this because it is in our interests to use this information to help run our business, or it may be to support a legal obligation we have.
Employee retention	Leave reasons, manager and employee evaluations, performance, role, position/title.	To understand why you left us. We do this because it is in our interests to use this information to help run our business or it may be to support a legal obligation we have.
Pension administration	Your contact details, compensation and benefits, years of service, payroll, and tax data.	To manage and administer your pension and related legal obligations.
Obligations to third parties	Your contact details, role, position, title, compensation & benefits.	To comply with our obligations to third parties in connection with your employment, such as tax authorities and professional bodies.

14. TRANSFER OF CONTROL

Data sharing in connection with a transfer of control



Circumstances may arise where we decide to reorganize or divest part (or all) of our business or a line of our business (or any portion of our assets). This can include our information databases and websites, through a sale, divestiture, merger, acquisition, in the event of a bankruptcy, or other means of transfer.

In such circumstances, your personal data may be shared with, sold, transferred, rented, licensed, or otherwise provided or made available by us or on our behalf to actual or potential parties to, and in connection with, the contemplated transaction (without your consent or any further notice to you). In such circumstances, we will seek written assurances that your personal data will be protected appropriately.

15. CHANGES TO THIS NOTICE



BMS may update its privacy notices from time to time. If there are any important revisions which might impact the way we process your personal data, BMS will notify you to inform you of these changes either directly or through our internal communication channels.

16. CONTACT US



If you have questions about this notice, or you want to obtain more information about our use of your personal data as a BMS Worker, you can ask a question by raising a ticket on myBMS. For current and previous employees, you can also contact us by email at eudpo@bms.com for the EU/EEA, Switzerland and the UK. If you are located in Australia, please email the team at contact.australia@bms.com or by post at the contact details as described on the relevant footer of our corporate websites that applies in your own language under the contact section.

You can find more information about data protection in your market below:

List of privacy notices for other jurisdictions					
Argentina	Australia	Austria	Belgium	Brazil	Canada
Chile	China	Colombia	Czech Republic	Denmark	Finland
France	Germany	Greece	Hong Kong	Hungary	India
Ireland	Israel	Italy	Japan	Korea	Luxembourg
Mexico	Netherlands	New Zealand	Norway	Peru	Poland
Portugal	Romania	Saudi Arabia	Singapore	Spain	Sweden
Switzerland	Taiwan	Thailand	Turkey	United Arab Emirates	United Kingdom