Last Reviewed Date: 08-March-2021
Effective Date: 08-March-2021

Merck & Co., Inc. (Kenilworth, NJ, USA) Notice of Data Practices for Employment- & Workplace-Related Purposes

The Purpose of this Notice

This Notice provides a comprehensive overview of the practices of Merck & Co., Inc. (Kenilworth, NJ, USA) and its affiliates with respect to the collection, use and disclosure of data for employment-related purposes about employees, their family members, job candidates, former employees, retirees, and other individuals about whom the Company and its affiliates have Personal Information as a result of the relationships those individuals have or had with the Company, or with employees of the Company.

This Notice is not intended to replace other notices or consents provided by our company or its affiliates to current or former employees or others in accordance with national and local laws and regulations or for specific programs. In the event of any conflict between notices or consents required by local law and this Notice, the notices or consents required by local law will prevail.

Consistent with our tradition of upholding high ethical standards across our business practices, we have demonstrated our commitment to privacy by establishing a global privacy program to support compliance with applicable privacy laws and standards for protecting personal information around the world.

Why We Collect Personal Information

As a global company, we continue to determine that important business efficiencies can be achieved by consolidating information about our employees, family members, and other individuals about whom the company has personal information, as a result of the relationships those individuals have with employees (the "HR data") in centralized databases and systems located at our facilities in the USA or with third parties who host applications for us. The primary company system of record for HR data is Workday. Workday also shares HR data with other systems and databases hosted by or on behalf of our company; however, Workday and those other systems and databases will only collect, receive, use and share HR data in accordance with and as permitted by applicable laws, our Global Cross Border Privacy Rules Policy, which is available at https://www.msdprivacy.com/us/en/cross-border-privacy-policy-rules.html (and includes our Binding Corporate Rules), and, where applicable, as authorized by applicable government authorities, in connection with employment-related activities, which may include:

- attracting and recruiting job candidate (e.g., job advertisements and postings, CV/resume reviews, applications, selection processes and platforms)
- skills, developmental, and leadership assessments
- organizational design and workforce planning (e.g. headcount planning, restructurings, employee movements, succession planning, terminations)
- budget planning and administration
- compensation, payroll, and benefits planning and administration (e.g., salary, tax withholding, tax equalization, awards, insurance and pension)
- workforce development, talent management, education, training and certification
- background checks
- performance management
- problem resolution (e.g., internal reviews, grievances), internal investigations, auditing, compliance, risk management and security purposes

- authorizing, granting, administering, monitoring and terminating access to or use of company systems, facilities, records, property and infrastructure
- business travel (e.g., limousines, commercial flights, company aviation services, hotels, rental cars)
- expense management (e.g., corporate card, expense and grant of authority administration, procurement)
- project management and planning of project assignments and resources
- conflict of interest reporting
- employee communications
- flexible work arrangements
- administration of employee enrollment and participation in activities and programs offered to eligible employees (e.g., matching donations to non-profit organizations, political action committee contributions, wellness activities)
- work-related injury and illness reporting
- monitoring and surveillance for industrial hygiene, public health and safety
- response to emergencies (e.g. natural disasters, national security, public health), crisis management and business continuity planning
- legal proceedings , government investigations, and audits including preservation of relevant data
- as required or expressly authorized by laws or regulations applicable to our business globally or by government agencies that oversee our business globally
- conduct workforce analytics as expressly authorized by law or regulation
- termination and offboarding procedures, such as providing supervisor temporary access to employee files and folders (e.g., OneDrive) on Company-issued devices, for the purposes of planning transition and continuity of work and preventing undue risk to operations.

Depending on the location in which you live, local laws may require that you provide specific consent for the collection, use and disclosure of HR data for some of these purposes. Where required, you may be asked to provide your consent by appropriate and permitted means.

What Personal Information We Collect

The types of HR data we collect (directly from individuals or from public or third party information sources) and share depend on the nature of your position and role within our Company and the requirements of applicable laws. Examples of this information, the legal basis for collecting and holding such information, and a description of why it is needed, may include, among other things the items in the following chart.

Note regarding sensitive data: (e.g., data that reveal race, ethnic origin, religious or philosophical beliefs, health, sexual orientation, political opinions or trade union membership) such data are collected only where required by law and are used and disclosed only to fulfill legal requirements or upon your specific request.

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
Contact information (e.g., name, home and business addresses, telephone, fax and mobile device numbers, e-mail addresses)	Performance of employment contract	To enable contact and communications between you and your employer
Date of birth	Performance of employment contract	For minimum wage purposes, redundancy calculations, rest break requirements and pension related purposes

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
Terms and conditions of your employment	Legal obligation	To ensure the Company upholds the terms and conditions of your employment contract
Bank account details	Performance of employment contract	To enable payroll
National identity number	Performance of employment contract	To enable payroll, various national insurance and medical plan deductions, and enable international assignments and transfers
Details of periods of sick leave	Compliance with a legal obligation	To enable payment of governmental statutory sick leave, where appropriate
Details of periods of sickness	Performance of employment contract	To enable payment of Company-funded sick leave, where appropriate
Nationality	Compliance with a legal obligation	Confirm eligibility status of employees
Disability status	Legitimate interest	In order to make reasonable adjustments to support the employee and tracking of diveristy and workforce objectives
Diversity data and equal opportunities monitoring information (e.g., ethnic origin, sexual orientation, religion, gender, etc.)	Compliance with a legal obligation	Tracking of workforce diversity objectives, where required
Details of qualifications / skills or employment history, including references from previous employers	Legitimate interest	To record competencies and qualifications obtained relating to one's job
Grievance records, and reports of potential compliance violations	Legitimate interest	To record any grievances or grievance investigations that have been carried out in relation to the employee (or raised by the employee), and to record agreed outcomes in the employment context
Disciplinary records	Legitimate interest	To record any investigations that have been carried out in relation to the employee in the employment context
Performance management records	Legitimate interest	To record any performance ratings, reviews, and other performance outcomes and support pay and promotion discussions
Timekeeping and attendance	Legal obligation	Ensure compliance with time recording requirements, where applicable
Home Contact details of next of kin and / or emergency contacts	Legitimate interest	To make contact in case of emergency
Monitoring in furtherance of health and safety (e.g., industrial hygiene exposure	Legitimate interest	To help monitor the safety of employees and others on-site, where applicable

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
assessment, noise dosimetry results, etc.)		
Contact details and personal data related to the use of IT systems (email, ISID, IP address, other online identifiers, etc.)	Legitimate interest	Administering Company applications, software, and systems to ensure that our systems are secure and are fit for use
Contact details and personal data related to the use and access to IT systems (name, email, ISID, etc.)	Performance of employment contract	In order to ensure the integrity and security of the Company's IT systems, protect Company assets and persons including employees' own privacy, certain monitoring will occur to prevent data loss, cyber-attacks or the introduction of malware or spyware. In addition, certain processing of personal information may take place by way of either persistent and/or session cookies in order to enhance the quality and simplify the use of our IT systems. Such processing is allowed by most legislation, including the EU General Data Protection Regulation (EC (No.) 2016/679), on the basis of legitimate interest.
Personal data related to files and documents stored in company-issued locations and drives, such as OneDrive.	Legitimate interest	To ensure proper business continuity planning of work upon end of employment and prevention of undue disruption of operations.

How and When Personal Information May be Shared with Our Partners

In the section below, we list the reasons that we typically may share HR data for employment-related purposes, the reasons that we may share this information, and whether you can limit this sharing. We implement reasonable and appropriate security measures to protect personal information in accordance with its sensitivity from loss, misuse and unauthorized access, disclosure, alteration or destruction.

Reasons Your Personal Information May be Shared for Employment Purposes	Do we share?	Can you limit the sharing?
Reporting to government authorities.	Yes, for example, to report safety information about our products.	No
To parties in relevant legal proceedings as authorized by the presiding court or tribunal and otherwise to the extent required or explicitly authorized by applicable law.	Yes	No, except where required by local law.

Reasons Your Personal Information May be Shared for Employment Purposes	Do we share?	Can you limit the sharing?
In the event that for business reasons we decide to divest part or all of our business through sale, merger or acquisition, to actual or prospective purchasers	Yes, based on written agreements that personal information will be protected appropriately in these circumstances.	Generally, no, except where local law permits you to opt-out or requires your express consent.
With companies globally that provide services on our behalf and in accordance with our instructions (for example, to deliver specific information you have requested)	Yes, if the business operation is supported by another company. As a global company, we may work with companies around the world to provide services for or on our behalf, and we will require those companies to protect personal information in accordance with applicable laws, rules and regulations and Company privacy policies.	Generally, no. We have instituted policy, contractual and administrative mechanisms requiring protection of personal information by other companies that process personal information on our behalf globally. However, where local law provides a right for you to limit this sharing, we will comply with such requirements. In circumstances where our business operations are supported by other companies, such as a company that we contract with to mail the materials you request, you will not be able to limit this sharing and still receive the service.
To affiliates* within the Merck & Co., Inc. (Kenilworth, NJ, USA) family of companies globally for everyday business purposes as described in this notice **Affiliates are companies related by common ownership or control. Outside of the United States and Canada, affiliates of Merck & Co., Inc. (Kenilworth, NJ, USA) generally operate under the names "MSD" or "Merck Sharp & Dohme"*	Yes, as a global company, we generally share personal information across our offices globally for the purposes described in this notice, however, only those individuals with a legitimate business need to access personal information for these purposes are granted such access. For example, HR data about you will be available to your management, who may be located in another country, the HR Business Partners responsible for your country and the HR centers located in the U.S.A. or regionally that are responsible for certain HR functions, such as compensation and benefits planning.	Generally, no. We have instituted policy, contractual and administrative mechanisms requiring protection of personal information across our business globally. One example of this is obtaining approval within the European Union of our Binding Corporate Rules. In exchange for internally applying the provisions of the General Data Protection Regulation, the Company is permitted to transfer information among all of its affiliates globally. However, where local law provides a right for you to limit this sharing, we will comply with such requirements.

Reasons Your Personal Information May be Shared for Employment Purposes	Do we share?	Can you limit the sharing?
To companies we collaborate with to use for their own products and services	When we collaborate with a third party to provide a service to our Company, the Data Processing Agreement between our Company and the third party strictly limits the processing of the HR data we share to only what is necessary to perform the service. The Data Processing Agreement prohibits third parties from using the HR data for any other purpose. In rare cases, third parties who may wish to provide product and services to individuals for other purposes outside of the Data Processing Agreement, will not be acting on behalf of our Company, nor will they be permitted to use the employee data we share with them to establish contact, but rather will need to seek the express consent of those individuals.	Yes
To other companies we collaborate with solely for activities related to products or services jointly offered or developed by us and that company.	Yes, subject to written agreements between us and those companies, which require those companies to protect confidential information provided to them by us.	Yes, where permitted by law. If you request to opt-out of this sharing, however, you will not be able to work on co-development projects that we undertake with such companies.
To internal employees with direct supervisory or managerial responsibility for employees.	Yes, subject to local laws and policies, managers are granted access to employee files and drives (i.e. OneDrive) to ensure proper work transition of former colleague's responsibilities and to avoid risk to operations.	While such business continuity procedures are required to ensure proper handoff of work, you can limit the personal information you store in Company drives and folders by choosing not to store personal documents on drives such as OneDrive or storing personal files in a single location where they can be

Reasons Your Personal Information May be Shared for Employment Purposes	Do we share?	Can you limit the sharing?
		easily deleted as you plan your offboarding from the Company.

How We Ensure the Security of Your Personal Information

We will take reasonable steps to protect your personal information, according to its sensitivity, how it is collected and transmitted between your computer or device and our online resources and servers, as well as to protect personal information in our possession from unauthorized access, disclosure, alteration or destruction. It is your personal responsibility to secure your own copies of your passwords and related access codes for our online resources. The Company's Information Security Standards Handbook sets forth the specific requirements for ensuring that the type and level of security is appropriate to the sensitivity of the information and the risk level of the activity, taking into account current technology best practices and the cost of implementation.

For How Long We Retain Your Personal Information

We generally retain personal information for as long as reasonably needed for the specific business purpose or purposes for which it was collected and the duration of your employment, use of company systems, apps and other relevant information assets. In some cases, we may be required to retain information for a longer period of time based on laws or regulations that apply to our business, such as applicable rules on statute of limitations or for other necessary business purposes. Where possible, we aim to anonymize the information or remove unnecessary identifiers from records that we may need to keep for periods beyond the original retention period. Details about retentions can be found in our Company Retention Policy.

Your Rights

In addition to the right to access or correct information, you may be entitled, in accordance with applicable law, to object to or request the restriction of processing of your personal information, and to request erasure of your own personal information. Requests should be submitted by contacting the Global Privacy Office (contact information below).

If you have additional concerns with our use of your personal information or our response to any exercise of your rights, you have the possibility to lodge a complaint to your local Data Protection Supervisory Authority.

Information on Our Company's Privacy Certifications and Commitments

The privacy practices of Merck & Co., Inc. (Kenilworth, NJ, USA) – also known as Merck Sharp & Dohme (MSD) outside of the U.S. and Canada - described in this Privacy Notice, comply with the APEC Cross Border Privacy Rules System, our Binding Corporate Rules (BCRs), which have been approved in the European Union, and our self-certification to the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield.

<u>EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield</u>

Merck & Co., Inc. (Kenilworth, NJ, USA) – also known as Merck Sharp & Dohme (MSD) outside of the U.S. and Canada - participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all personal data received from European Economic Area (EEA) member countries, the United Kingdom, and Switzerland, in reliance on each Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and

to view our certification, visit the U.S. Department of Commerce's Privacy Shield List. [https://www.privacyshield.gov/list]

We are responsible for the processing of personal data we receive, under each Privacy Shield Framework, and subsequently transfer to a third party acting as an agent. We comply with the Privacy Shield Principles for all onward transfers of personal data from the EEA, UK, and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Click here to check our Privacy Shield verification status.

Merck & Co., Inc. (Kenilworth, NJ, USA) – also known as Merck Sharp & Dohme (MSD) outside of the U.S. and Canada - has further committed to cooperate with the EU Data Protection Authorities (DPAs) for EEA employees, and the Swiss Federal Data Protection and Information Commissioner for Swiss employees, with regard to unresolved Privacy Shield complaints concerning HR data transferred from the EU or Switzerland, respectively, in the context of the employment relationship.

Under certain conditions, more fully described on the Privacy Shield website [https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint], you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

APEC Cross Border Privacy Rules System

The APEC CBPR system provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. More information about the APEC framework, Binding Corporate Rules and EU-US Privacy Shield can be found here; https://www.msdprivacy.com/us/en/index.html. You can click here to view our APEC CBPR certification status.

Contact Our Global Privacy Office

If you have questions regarding this notice or the personal information we collect, use and share about you, or if you would like to access or update personal information about you in our databases in accordance with your rights under applicable law, please contact us. To contact the Global Privacy Office,

- Write to:
  Global Privacy Office
  Merck & Co., Inc. UG4B-24
  351 N. Sumneytown Pike North Wales, PA, USA 19454
- Send an e-mail to: Global Privacy Office

We reserve the right to modify, add or remove portions of this notice at any time. If we decide to change this notice, we will post the updated notice on our web site, prior to the changes becoming effective, at https://www.msdprivacy.com/us/en/transparency-and-privacy.html.