Effective Date: 1 June 2021

Organon & Co. (Jersey City, NJ, USA)
Notice of Data Practices for Employment & Workplace-Related Purposes in Canada

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.

The Purpose of this Notice

This Notice provides an overview of the practices of Organon & Co., (Jersey City, NJ, USA) and its affiliates with respect to the collection, use and disclosure of personal data for employment or work-related purposes. This includes Personal Information about employees, their family members, former employees, retirees and other individuals about whom the Company and its affiliates may have data as a result of the relationships those individuals have or had with 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.

Why We Collect Personal Information

The Company collects Personal Information of its current and past employees, their family members and individuals that had a working relationship with the Company for purposes of administering various human resources worker-related programs ("HR Data"). The HR Data collected from these individuals are transferred to the United States, where the Company is headquartered. The Company has engaged a trusted third party to store the HR Data in an approved system of record. Other systems and databases hosted by or on behalf of our Company may have access to the HR Data; however, those 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, and where applicable, as authorized by government authorities. The HR Data is processed for employment or work-related activities including, but not limited to:

- attracting and recruiting job applicants (e.g., job advertisements and postings, Curriculum Vitae/resume reviews, applications, selection processes)
- skills, developmental, and leadership assessments
- organizational design and development and workforce management (e.g., headcount planning, restructurings, employee movements, succession planning, terminations)
- budget planning and administration
- compensation, payroll, and benefit 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
- emergencies (e.g., natural disasters, national security, public health) and our response, 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 human resources data for some of these purposes. Where required, you may be asked to provide your consent by appropriate and permitted means.

To ensure the integrity and security of the Company's IT system, such as to prevent data loss, cyberattacks or the introduction of malware or spyware, and to protect Company assets and workforce, certain monitoring will occur on Company devices and in Company facilities. 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 or in conformity with local legislation.

What Personal Information We Collect

The types of HR Data we collect (directly from you 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: sensitive data, data that reveal race, ethnic origin, religious or philosophical beliefs, health, sexual orientation, political opinions, or trade union membership, are collected only where required by law and are used and disclosed only to fulfill legal requirements or upon your specific consent.

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
Personal identifiers, such as name, nickname or alias, home and business addresses, telephone, cellphone, and fax numbers, personal and business	Fulfillment of employment relationship	To enable contact and communications between you and your employer, allowing your employer to appropriately manage the work environment

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
e-mail addresses, written or electronic signatures, IP address)		To enable payroll, various national insurance and medical plan deductions, and enable international travel, assignments, or transfers
Date of birth	Fulfillment of employment relationship	For social security and similar tax calculations, proper administration of benefits plans, minimum wage purposes, redundancy calculations, rest break requirements and pension related purposes
Terms and conditions of your employment	Compliance with a legal obligation	To ensure the Company upholds the terms and conditions of your employment contract
Banking information, such as bank account number and routing details	Fulfillment of employment relationship	To enable timely compensation payments
Details of period of sick leave	Compliance with a legal obligation	To enable payment of governmental statutory sick leave, where appropriate
Details of periods of sickness	Fulfillment of employment relationship	To enable payment of Company-funded sick leave, where appropriate
Nationality	Compliance with a legal obligation	Confirm work eligibility status of employees
Disability status	Fulfillment of employment relationship and/or compliance with a legal obligation	In order to make reasonable adjustments to support the employee and tracking of equal opportunities
Diversity data and equal opportunities monitoring information (e.g., ethnic origin, sexual orientation, religion, gender, etc.)	Compliance with a legal obligation	Tracking of equal opportunities and diversity targets, where required
Details of qualifications / skills or employment history, including references from previous employers	Fulfillment of employment relationship	To record competencies and qualifications obtained relating to the individual's job
Grievance records	Fulfillment of employment relationship	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	Fulfillment of employment relationship	To record any investigations and subsequent actions that have been carried out in relation to the employee in the employment context

Personal Information Collected	Legal Basis for Holding the Information	Description of Why the Information is Needed
Performance management records	Fulfillment of employment relationship	To record any performance ratings, reviews, and other performance outcomes and to support pay and promotion discussions
Timekeeping and attendance	Compliance with a legal obligation	Ensure compliance with time recording requirements, where applicable
Contact details of next of kin and / or emergency contacts	Fulfillment of employment relationship	To make contact in case of emergency
Monitoring in furtherance of health and safety (e.g., industrial hygiene exposure assessment, noise dosimetry results, etc.)	Fulfillment of employment relationship and/or compliance with a legal obligation	To help monitor the safety of employees and other workers on-site, where applicable
Contact details and personal data related to the use of IT systems (email, ISID, IP address, other online identifiers, etc.)	Fulfillment of employment relationship.	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.)	Fulfillment of employment relationship	Authorizing, granting, administering, monitoring and terminating access to or use of Company systems, facilities, records, property and infrastructure.
Personal data related to files and documents stored in company-issued locations and drives, such as OneDrive.	Fulfillment of employment relationship and/or compliance with a legal obligation	To ensure proper business continuity, planning of work upon end of employment or assignment 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 work related purposes, 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 Work 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 allowed by local law.
To actual or prospective purchasers, in the event the Company decides to divest part or all of our business operations	Yes, based on written agreements that personal information will be protected	Generally, no, except where local law permits you to opt-out or requires your express consent.

Reasons Your Personal Information May be Shared for Work Purposes	Do we share?	Can you limit the sharing?
through sale, merger or acquisition,	appropriately in these circumstances.	
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, to a company that is supporting the particular business activity for which your personal information is needed. 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 foryou to limit this sharing, we will comply with such requirements. Incircumstances where our business operations are supported by other companies, such as a company that we contract with to mail the materials you request, if you limit this sharing, you will not be able to still receive the service.
To affiliates* within the Organon & Co. (Jersey City, NJ, USA) family of companies globally for everyday business purposes as described in this notice **Affiliates are companies related by common ownership or control.*	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 to allow the sharing of such information for legitimate business purposes. However, where local law provides a right for you to limit this sharing, we will comply with such requirements.
To companies we collaborate with to use for their own products and services	In rare cases, companies with whom we collaborate, but who are not acting on our behalf, may request that we share HR data so	Yes

Reasons Your Personal Information May be Shared for Work Purposes	Do we share?	Can you limit the sharing?
	that they can provide information about their own products and services to you. In such a case we would only share information about you if you provide your express (opt-in) permission for this sharing.	
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 or external workers who are terminating their employment or assignments with the Company.	Yes, subject to local laws and policies, managers are granted access to employee or external worker 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 easily deleted as you plan your offboarding from the Company.

How We Ensure the Security of Your Personal Information

We take reasonable steps to protect your personal information, according to its sensitivity, and how it is collected and transmitted between your computer or device and our online resources and servers. These safeguards aim to protect personal information in our possession or control 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 or as permitted by law for the specific business purpose or purposes for which it was collected and for your use of company systems, apps and other relevant information assets. We consider the following criteria in determining the proper retention period for your personal information: (i) our working relationship with you; (ii) whether we have a legal or regulatory obligation to which we are subject; and (iii) whether retention is advisable in light of applicable statutes of limitations, or for the defense or prosecution of legal claims, or regulatory investigations. 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. Where possible, we aim to deidentify or pseudonymize the information or remove unnecessary identifiers from records that we may need to keep for periods beyond the original retention period. Details about retention schedules 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 local law, to object to or request the restriction of processing of your personal information, request erasure of your own personal information, or request a copy of your data. 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 option to lodge a complaint with your local data protection authority.

Information on Our Company's Privacy Certifications and Commitments

The privacy practices of Organon & Co. (Jersey City, NJ, USA) described in this Privacy Notice, comply with the 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 can be found here. 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:

Organon Global Privacy Office
30 Hudson Street
Jersey City, NJ 07302

or

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 http://www.organon.com/privacy.