Review Date: 16 May 2022
Effective Date: 23 May 2022

ORGANON PRIVACY NOTICE

1. ORGANON – WHO WE ARE AND WHAT WE DO

Organon, (hereafter, "**us**," "**we**" and (the) "**Company**") is a global healthcare company focused on improving the health of women throughout their lives. We develop and deliver innovative health solutions through a portfolio of prescription therapies, biosimilars, and established brands. Our online resources provide health, medical, and product-related information, employment, and other information related to our business. In addition, some of Organon's online resources enable qualified professionals to apply for grants or contribute to research studies or make purchases on-line. In this document, all our relevant activities and offerings are collectively referred to as "**Products and Services**."

We have adopted this privacy policy ("**Privacy Notice**") to help you understand what types of Personal Information (defined below) we collect and process in connection with providing the Products and Services, how and, why we do so, who may have access to that information and what your choices and individual rights are for that information (collectively, "**Privacy Practices**"). This Privacy Notice covers the Privacy Practices of Organon, its U.S. based subsidiaries and affiliates[1], and spells out the principles of our global privacy practices.

The Company has subsidiaries and affiliates in a large number of geographies across the globe. Many of those states and countries have specific privacy laws that may impose different or additional requirements than those underlying this Privacy Notice (collectively, **"Data Protection Laws**"). Please refer to the list of non-U.S. Organon companies accessible here to access to their privacy policies. Unless a Company affiliate has posted its own Privacy Notice, the terms of this notice apply to the Privacy Practices of that entity.

2. WHAT IS COVERED BY THIS NOTICE?

This Privacy Notice applies to our Privacy Practices with respect to Personal Information collected by us off-line and online. For example, when you visit our offices or other facilities (**"Sites**") or use our websites, mobile applications (apps) e-mail, and other online and downloadable tools) that display a link to this Notice. In certain cases, we may give you a Special Privacy Notice when you interact with us, participate in, or use, our Products or Services, for example if you are an employee or a Health Care Provider ("**HCP**"). As any such Special Notice applies to specific interactions with you, any of its terms that differ from this Privacy Notice will control.

[1] Organon Canada Holdings LLC, Organon Global Inc., Organon LLC, Organon Pharma Holdings LLC, Organon Trade LLC, and Organon USA LLC.

This Notice does not apply to third-party online resources to which our websites may link, where we do not control the content or the privacy practices of such resources.

Definitions and Glossary

In order to streamline this policy, we are using a number of defined terms (capitalized nouns) and technical concepts. To help you to become familiar with those terms to the extent that they are not explained on this page, we have created a Glossary of Privacy Terms.

"**Personal Information or Personal Data**," as used in this Privacy Notice, means (i) information relating to an identified or identifiable natural person, including data that identifies an individual or that could be used to identify, locate, track, or contact an individual. Personal Information includes both directly identifiable information such as a name, identification number or unique job title, and indirectly identifiable information such as date of birth, unique mobile or wearable device identifier, telephone number as well as key-coded data, online identifiers such as IP addresses or any personal activities, behavior, or preferences which may be collected to provide services or products and (ii) any other information that constitutes "personal information", "personally identifiable information", "personal data", or any similar category of protected personal information or data under applicable Data Protection Laws.

In this Policy we are using the terms **"collecting**" and **"processing**" Personal Information interchangeably. In each case, this means any operation or set of operations on PI, whether or not by automatic means, including, but not limited to, collecting, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, evaluation, analysis, reporting, sharing, disclosure, dissemination, transmission, making available, alignment, combination, blocking, deleting, erasure or destruction

We refer to "**Customer(s)**" as individuals whose Personal Information we have collected and hold in an identifiable structured format, such as user accounts, and who are not employees, contractors, shareholders, officers, directors and agents or any Company entity.

3. PERSONAL INFORMATION WE COLLECT AND HOW WE USE IT

Organon is committed to ensure that its Privacy Practices are fair, lawful, and transparent. We are committed to building and preserving the trust of our customers, partners in business, medical professionals, and our employees by respecting individual privacy expectations, working to prevent privacy harms, and fostering compliance with data protection laws around the world.

Please review our Privacy Notice and the documents mentioned in it before disclosing Personal Information to us. If you have questions or concerns with respect to our Privacy Practices, please contact us. The contact information for the privacy office in charge of your region can be found here.

Categories of Personal Information we Collect

We collect the following categories of Personal Information:

Personal Identifiers

We collect personal identifiers such as:

- Names, mailing addresses, email account names and addresses, social media account names, online identifiers, such as Internet Protocol Addresses and similar identifiers whenever you interact with us on-line, we respond to an inquiry, or you use our Product or Services.

- We may also collect some of that information when you interact with us in person, e.g., when visiting one of our Sites, interact in person with Organon personnel (e.g., field representatives, or Organon booths on trade shows and conferences) or interview for a job.

- If warranted by circumstances, for example, if we need to verify your identity as a job applicant or service provider, or to comply with tax and reporting requirements, we could also collect your driver's license or social security or individual taxpayer number or passport information, or your car's license plate number if you are entering our premises.

We collect personal identifiers primarily whenever we need to be able to contact you or to verify your identity, to deliver services or products, interview or hire you for a job, manage an employment or contractual relationship with you, advertise our Products or Services, form a better understanding about your interests, personal characteristics, and preferences, and to grow, operate and protect our business in general.

We collect personal identifiers on-line and off-line. We collect that information directly from you, for example when you are filling out contact forms on our website or apps supplied by us. In many instances, we collect such personal identifiers indirectly through the use of technology when you interact with us online. We also may collect personal identifiers by using public information such as publicly available government data bases, data brokers, internet analytics providers and social media.

Other Identifying Information

In addition to the personal identifiers mentioned above, we are also collecting the following types of identifying information:

- Education and employment history- if you are applying for a job or if you are a medical professional with whom we engage, e.g., as a speaker at a conference

- Financial account information- including banking details in order to pay you a salary or for goods and services you supply.

- Credit and debit card information to process payment if you are a Healthcare Provider and order products from us online. We use this information to verify the validity of the credit/debit card information with financial institutions and to process payments. We collect credit /debit card related information directly from you to process those orders and we may also use external approved third parties (i.e., on-line credit card checking managed by financial or credit organizations).

- Health insurance information and medical information- in connection with patient surveys and payment assistance programs.

Sensitive Information

Some of the Personal Information we collect is sensitive and classified as protected by applicable law and/or Special Categories of Data under EEA/UK data protection law. We collect that type of information primarily in the context of employment applications and relationships, administration of benefits and to meet legal reporting requirements.

Those data types include age (over 40), trade-union membership, race, color, ancestry, national origin, immigration status (citizenship), marital status, disability, gender, veteran and military status, sexual orientation, and gender expression. Unless we need to collect those types of Personal Information to meet legal obligations, the disclosure of this information is voluntary.

We are also collecting health-related information about our customers, employees and others provided to us when responding to questions and surveys or through use of online and downloadable health-related tools we provide. Those data may include diagnostic information and information about symptoms commonly associated with illness.

We treat this information as sensitive and restrict processing and access. We will collect those types of Personal Information only in compliance with all legal requirements in case the applicable Data Protection Laws of your country of residence, such as GDPR for EEA residents, impose additional conditions for processing such data.

Biometric Information

Certain Sensitive Information (see above) collected by us may include biometric information forming part of diagnostic information collected by us in order to assess our Products or Services. We obtain consent prior to collecting or using biometric information.

Internet or Electronic Network Activity Information

- Information Collected from your Computer or Other Electronic Devices

  We collect information about your computer or other electronic device when you visit our websites and use our online resources. This information may include your Internet Protocol (IP) address, Internet Service Provider (ISP), domain name, browser type, date and time of your request and information provided by tracking technologies, such as cookies, single-pixel tags, local share objects (Flash), local storage, etags and scripts.

  We collect such Personal Information online as necessary to enable individuals to register for, customize and personalize certain of our online resources and communications. We use Personal Information collected online to provide products, services and features and other resources that individuals have requested; for example, educational literature and related information about our business, e-mail programs, tools, quizzes, questionnaires, and

surveys. We analyze Personal Information collected online to identify and offer additional services and promotions that we believe you might find interesting. We may evaluate use of some online resources and communications but do so with non-identifiable or aggregate information only. We also may use Personal Information to audit our online resources for compliance, authorized access, and security.

We and the third parties that provide content, functionality or services on our online resources may collect information about you and/or your device by using cookies or similar tracking technologies to serve advertisements to your computer or other electronic device or to remind you about our website that you previously visited. Please see our Global Online Tracking Policy for more information about cookies and related technologies and how you can control them. If you use a mobile device to access our websites and online resources or to download our mobile apps or services, we also may collect information about your device, such as your device ID and device type, as well as usage information about your device and your use of our mobile websites and other mobile resources.

- Social Media

We collect Personal Information to enable you to use online social media resources we may offer from time to time. Examples of social media resources include social networks, discussion boards, bulletin boards, blogs, wikis, and referral functions to share content or tools with a friend or colleague. We may also enable you to use these social media resources to post or share Personal Information with others. You should consider carefully what information you choose to share about yourself and others such as colleagues, friends, customers, or patients, when you use social media resources. By providing us with the information of another individual, you represent that you have the authority to do so.

Sensory Information

We collect audio and video information that represents Personal Information, e.g., when we are using security cameras to monitor premises or other critical infrastructure controlled by us or if we record certain phone conversations with third parties for training or quality control purposes or to comply with legal obligations. We may also record video messages for marketing purposes or as part of our engagement with Healthcare Professionals. In all instances, we strive to give affected individuals adequate prior notice, and obtain, where required, consent before collecting such information.

Professional and Employment Related Information

- Recruitment:

We collect Personal Information about the educational history of potential and actual job candidates, such as, including schools attended, grades and scores, fields of study, degrees obtained and graduation dates, interests, skills and hobbies, professional licenses and certifications, publications, and other professionally relevant public contributions.

We also collect Personal Information connected with the employment history of actual and potential job candidates, including names of employers, supervisors, location, and date of employment, where permitted, salary history and promotions, and other Personal Information that may help us evaluate the suitability of a candidate for a specific position.

If you apply for a specific position or submit a general application, we collect also certain types of Sensitive Information. This occurs on a voluntary basis unless collection is legally required. As the laws of states and countries where we recruit and applicable Data Protection Laws may contain additional requirements, we strive to provide job candidates with a special privacy notice detailing all applicable privacy practices. Details regarding our HR related privacy practices can be found in our special Notice of Data Practices for Employment and Workplace Related Purposes.

- Engagement with Professionals

We collect Personal Information about health care professionals who register on our web=sites or may collaborate with us, including their medical specializations, organizational and institutional affiliations, patents awarded or other scientific achievements directly or from public or third-party information sources to verify their professional credentials, achievements, and identity. For details, please see our Notice of Data Practices for Health Care Professionals.

Inferences Drawn from any Type of Personal Information Used for Profiling, Consolidation

- Social Media Listening

Social media listening is the process by which we identify and assess what is being said about a company, individual, product or brand on the Internet. We only collect proportionally reasonable, relevant, and adequate, publicly- available Personal Information. If your Personal Information is collected for processing beyond the original intent when you posted the content, reasonable efforts will be made to provide notice to you as soon as is practical. Reasonable efforts might entail identifying your contact details from the social media platform, if possible, or within the posting. Moreover, we will make reasonable efforts to provide you with a mechanism by which to opt-out of our proposed data processing or exercise your rights as required by our policy and applicable regulations. Because of the nature of social media, it may not always be possible for us to identify the individual and contact details of who posted the original content that we collect.

- Consolidation

In some cases, we consolidate Personal Information that we collect about individuals through various services and channels, such as the telephone, surveys, websites and other online resources and communications, in order to enhance the quality of services that we offer.

Sources of Personal Information

- Directly Obtained

Typically, we inform you prior to or at the point of collection that we are collecting Personal Information data about you. In case a display of an entire privacy notice is not feasible, we use other means, such as placing labels on devices or using visual displays to alert you to our data collection activities and to refer you to this or any other applicable privacy notice.

- Obtained from Third Parties and Public Sources

  If we obtain Personal Information about you that has been collected by an independent third party, we seek contractual assurances that such Personal Information has been collected in accordance with applicable legal requirements, such as providing you with the disclosures and notices required by applicable Data Protection laws and that any privacy rights you have under that law are respected.

  We also collect Personal Information from the public domain for adverse event reporting purposes to fulfill our pharmacovigilance compliance requirements. The legal basis for this type of collection of personal information is to satisfy a legal obligation. In these circumstances, no consent from you is required, but we will provide you with notice as part of our pharmacovigilance policies and procedures.

4. WHY DO WE COLLECT, USE AND SHARE PERSONAL INFORMATION?

We process Personal Information for pre-determined specific, explicit, legitimate disclosed and documented purposes. We will not process your Personal Information for other purposes that are incompatible with such disclosed purposes, unless we have met all applicable legal requirements, including providing you with any required notices.

We do not collect or process more Personal Information than is needed or retain it in identifiable form for longer than is needed for those defined business purposes and applicable legal requirements. We anonymize or deidentify the Personal Information when business needs require that data about an activity or process involving Personal Information to be retained for a longer period of time. We ensure that these necessity requirements are designed into any supporting technology and that they are communicated to third parties supporting the activity or process.

We have listed the typical business purposes for processing specific categories of Personal Information in our description of the categories of Personal Information we collect.

If new legitimate business purposes are identified for processing Personal Information that was collected at an earlier date, we either obtain the individual's consent for the new use of Personal Information, or we ensure that the new business purpose is compatible with, the purposes described in a privacy notice or other transparency mechanism that was previously provided to the individual.

We will determine compatibility based, among other things, on the context in which the information was collected, the reasonable expectations of the individual, and the nature of the Personal Information in question.

We do not apply this principle to anonymized or deidentified information, or where we use Personal Information solely for historical and scientific research purposes and (a) an Ethics Review Committee, or other competent reviewer, has determined that the risk of such use to privacy and other rights of individuals is acceptable, (b) we have put in place appropriate safeguards to ensure data minimization, (c) the personal data is pseudonymized and (d) all other applicable Data Protection Laws are respected.

5. LEGAL BASIS FOR PROCESSING

If you are a resident of an EEA country, the UK, or another state or country requiring that specific legal requirements must be met as a condition for lawfully processing Personal Information, we will process your Personal Information only in accordance with such requirements. As such requirements may vary from country to country, please refer to our GDPR Privacy page.

6. HOW WE KEEP PERSONAL INFORMATION ACCURATE AND SECURE

Data Security

We take reasonable steps to protect Personal Information, according to its sensitivity, proportionate to the risk associated with the underlying processing activity as it is collected and transmitted between your computer or device and our online resources and servers. You are responsible for securing your passwords and related access codes to our online resources.

We implement reasonable safeguards to protect Personal Information in our possession or control from loss, misuse, and unauthorized access exfiltration, theft, disclosure, alteration, or destruction. We have implemented a comprehensive information security program and apply security controls and safeguards that are based on the nature and sensitivity of the information and the risk level of the activity, taking into account current technology best practices. Our functional security policies include, but are not limited to, standards on business continuity and disaster recovery, encryption, identity and access management, information classification, information security incident management, network access control, physical security, and risk management.

Security Incidents and Personal Data Breaches

In the event that a Security Incident affecting your Personal Information processed by us involves an event qualifying as a Personal Data Breach, Personal Information Security Breach or similarly termed event by applicable Data Protection Laws, we will take reasonable measures to contain and mitigate such a breach and ascertain its harm to individuals whose Personal Information has been affected. Depending on the legal requirements of the state or country where the incident occurred, we will notify governmental authorities and affected individuals as may be required in each case.

Data Quality

We strive to maintain Personal Information accurate, complete, and current, consistent with its intended use. We ensure that periodic data review mechanisms are designed into supporting technologies to validate the data accuracy against source and downstream systems.

We ensure that Sensitive Information is validated as accurate and current prior to its use, evaluation, analysis, reporting or other processing that presents a risk of unfairness to people if inaccurate or outdated data are used.

7. HOW LONG WE KEEP PERSONAL INFORMATION

We retain Personal Information for as long as reasonably needed for the specific business purposes for which it was collected and the duration of your use of our sites, apps, and other relevant online tools. We consider the following criteria in determining the proper retention period for your Personal Information:

- our working relationship with you;
- whether we are subject to a legal or regulatory obligation;
- whether retention is advisable in light of applicable statutes of limitations, or for the defense or prosecution of legal claims, or regulatory investigations that apply to our business, 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.

8. WHO HAS ACCESS TO AND WITH WHOM WE SHARE PERSONAL INFORMATION?

Personal information about you will be accessible to the Company and its subsidiaries, divisions, and groups worldwide, and to individuals and organizations that use Personal Information solely to help us operate our business or at our direction only in accordance with this Notice and applicable Data Protection Laws. In any event, access to your Personal Information will be documented and permitted only on a need-to-know basis. All persons accessing Personal Information under this Policy will be bound by a statutory and/or contractual confidentiality obligation.

Moreover, processing of Personal Information by third parties acting on our behalf are governed by agreements that ensure the accountability of such Parties for compliance with the principles of this Notice and applicable Data Protection Laws.

Sharing of Personal Information with Third Parties

We are sharing Personal Information with third parties only to achieve lawful and predetermined business purposes. We will perform a third-party risk assessment to verify the suitability of the third party and to ensure that shared Personal Information is properly protected. We will seek contractual assurances that the third party will comply with our policies and the requirements of relevant Data Protection Laws, such as giving any required notices and respecting the rights of individuals with respect to the processing of their Personal Information.

- Use of Processors and Contractors

  If we are sharing Personal Information with third parties acting as service providers, business associates or data processors, we will do so only pursuant to a written agreement

that requires the third party to process Personal Information exclusively in accordance with our documented instructions. Third parties may process the Personal Information we share with them only for, and to the extent necessary to accomplish, the purposes specified in their agreement with us. We will require any Third Party we share Personal Information with to implement reasonable security measures to protect the shared Personal Information and to remain accountable for its use during and after the end of our contractual relationship.

- Sharing of Personal Information with Third Parties Other than Processors or Contractors

  We are sharing Personal Information with third parties who assist us with operating and growing our business. The categories of such third parties include business services providers, such as payroll companies, accounting and tax services providers, advertising, marketing and market research companies, companies distributing email-based advertisements and companies and institutions collaborating with or assisting us in pharmaceutical research and manufacturing and the distribution of therapeutics. Furthermore, we are sharing Personal Information with other businesses and service providers that assist us with providing, managing, and protecting our on-line resources and internal networks, systems, and other assets.

- Categories of Personal Information Shared, Purposes of Sharing

  We may share most categories of Personal Information collected about you with various third parties for the same defined purposes for which they have been collected. We will honor your request that we stop sharing your Personal Information to honor your choices in accordance with our policies and/or to comply with applicable Data Protection laws.

- No Selling of Personal Information

  We neither share your information with third parties for money or other valuable consideration (other than as part of a contract where they provide a service to us) nor sell your information for money or other valuable consideration.

- Third Party Access Requests, Legal Process

  We will be compelled to disclose Personal Information in response to third parties to comply with legal process and court orders or to government agencies to comply with orders to grant access to or produce information in the context of criminal and civil investigations, or if such a disclosure is necessary to comply with regulatory requirements.

  We will process and disclose Personal Information to protect or defend our rights, prevent or take action against illegal activities, suspected fraud or situations involving potential threats against the safety of persons.

- Business Transitions

  In the event that we sell or transfer all or a portion of our business or assets (including in the event of a reorganization, spin-off, dissolution or liquidation) or enter into joint-ventures

or other business combinations, the Personal Information held in connection with the part of our business or assets affected by the transaction will become accessible to third parties.

We aim to protect your Personal Information by assessing the privacy practices of the other business(es) involved in such a transaction as part of our decision to proceed with a transaction. We also endeavor to enter into agreements with the other business(es) involved in such a transaction to ensure the continued protection of your Personal Information consistent with our privacy policies.

9. INTERNATIONAL TRANSFERS OF PERSOANAL INFORMATION

If permitted by law, including applicable Data Protection Laws, we may store, access, or otherwise process your Personal Information in or from any location where we conduct business and where our service providers are located. Personal Information that is subject to GDPR or UK GDPR will be transferred outside of the EEA or the UK only in accordance with applicable EU and UK regulations. Any transfers of Personal Information between Organon entities and/or affiliates will be governed by an Intragroup Data Sharing Agreement.

International Transfers of Personal Information Subject to GDPR to "Third Countries"

In the event that Personal Information is collected or processed by an Organon entity subject to GDPR or UK GDPR or Swiss law, any transfer of such information to a recipient in a country other than an EEA country or the UK that has not been ruled to offer an adequate level of data protection will be carried out in accordance with the applicable GDPR requirements.

We assess periodically the conditions in countries where the recipients of Personal Information we may transfer are located. Based on those assessments, we implement together with the prospective recipients of Personal Information measures to ensure that an adequate level of protection is for transferred Personal Information is available.

For any new transfers of Personal Information to third parties, service providers and data processors we rely on legally recognized transfer mechanisms, such as the appropriate module of the EU Standard Contract Clauses (2021) or the corresponding instruments approved by the UK, the Swiss or the Serbian authorities. Alternatively, we may rely from time to time on other authorized transfer mechanisms, such as individual derogations under Art 49 GDPR.

APEC

Our privacy program and practices comply with the Asia Pacific Economic Cooperation (**"APEC**") Cross Border Privacy Rules system for transfers of personal information from APEC member states to, amongst other places, the United States. We work to implement and uphold consistent global privacy standards to provide assurance for how we manage our privacy and data protection obligations across countries and regions and to support our APEC Cross Border Privacy Rules certification

10. YOUR CHOICES ABOUT HOW WE COLLECT OR USE PERSONAL INFORMATION AND YOUR ABILITY TO ACCESS, CORRECT AND DELETE PERSONAL INFORMATION AS A CUSTOMER

Choices to Limit Collection of Personal Information or Online-Tracking

You have choices whether and how much Personal Information to disclose to us.

You may limit the collection of Personal Information by us. Many of our online resources are available to you without requiring you to enter any Personal Information into a form or data field. In that case we will only automatically collect certain information related to your device and the way you are accessing our resource. However, if you wish to use personalized services provided by our online resources, you will be typically required to identify yourself.

We respect your choices with respect to your communications preferences, also if you opt-out of communications you requested previously. Please use the opt out link provided in our electronic communications or by contacting us at this email: privacyoffice@organon.com.

Limitations and Options on Tracking

We and the third parties that provide content, functionality or services on our online resources collect information about you and/or your device by using cookies or similar tracking technologies to the extent necessary to ensure the quality and the safety of your user experience. You have choices, however, with respect our use of cookies and other tracking technologies used for serving you advertisements, analyzing the use of our online resources, or tracking your browsing habits cross various websites. You can control our use of certain tracking technologies, such as cookies, through most Internet browsers. They typically enable you to limit or disable the use of cookies for specific websites. When you access our online resources for the first time, a pop-up banner will allow you to reject or tailor the use of cookies and similar tracking technologies that are not essential for ensuring the quality and the safety of your user experience. For more details, please see our Global Online Tracking Policy. More information about cookies and similar technologies and the way to control them is available at

- Network Advertising Initiative at: http://www.networkadvertising.org/optout_nonppii.asp
- European Interactive Digital Advertising Alliance at: http://youronlinechoices.eu/

For more information on how to disable tracking for certain web browsers and mobile devices, visit http://allaboutdnt.com/ .

Rights Available to all Customers as a Matter of Company Policy

In keeping our commitment to privacy, we give all customers and other individual third parties whose Personal Information we have collected and hold in an identifiable structured format, such as user accounts ("**Customer**"), a variety of choices with respect to such data. For the avoidance of doubt,

this Section does not apply to employees, contractors, shareholders, officers, directors, and agents or any of our entities.

Any commitments to Customers made in this Section are subject to any limitations imposed by applicable local laws and the following restrictions:

Except where prohibited by law, we may deny a Customer request in case a particular request would impede us in its ability to:

- comply with a law or an ethical obligation, including where we are required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements,
- investigate, make, or defend legal claims,
- perform contracts, administer relationships, or engage in other permitted business activities and were entered into in reliance on the information about people in question, and
- result in disclosure of Personal Information about a third party, result in breach of a contract, or in disclosure of trade secrets or other proprietary business information belonging to us or a third party.

The options for Customers to access, correct and request the deletion of their Personal Information described in this Section are in addition to any Data Subject Rights or Consumer Rights available under applicable Data Protection Laws.

We will deal with your request in the course of our normal business operations. For details, please see how we process any inquiries and complaints.

- Access to Personal Information

  We will address any Customer request for information about the Personal Information collected about you by a specific entity controlled by us. We will either inform you about the categories of Personal Information collected within the last year or provide you with specific pieces of Personal Information in a readable format covering that period.

- Correction of Inaccurate Personal Information

  We will honor Customer requests to correct inaccurate Personal Information that we are actively using, such as contact information or payment information. We may require Customers to back-up any alleged inaccuracy by independent documentation. Where offered, you also may update Personal Information about you online by modifying information that you previously have entered into forms or data items in fields on our websites

- Deletion of Personal Information

Personal Information should be stored only as long as it is necessary to be retained for a specific purpose. We will honor Customer requests to delete their Personal Information in a manner that it cannot be any longer reasonably linked to an identifiable individual. Depending on the nature of the data the deletion of which is requested, we may have to use additional measures to verify your identity and your authorization to dispose of the data. For operational reasons, implementation of a deletion request may have to be synchronized with the data maintenance cycles of the relevant storage media and providers. Customers should be aware that local Data Protection Laws frequently impose additional restrictions and exceptions in connection with Customer data deletion requests.

- Withdrawal of Consent, Opting out from Use of Personal Information for Marketing and Automated Decision-Making

We honor Customer requests to opt-out from the further processing of their Personal Information in cases in which

- they had originally given their consent to such processing. Examples would include as unsubscribing from newsletters or ceasing to participate in programs and activities.
- Personal Information collected about them is used for direct marketing communications,
- Personal Information collected about them is used to evaluate or to make decisions about them and (i) such decisions have the potential to significantly affect them and (ii) are made solely by use of automation or algorithms.

The link to the website where you can exercise your privacy rights in your respective country can be found here.

Note that in some cases, like social media listening, we are not the initial publisher of the Personal Information we may collect. We will do our best effort to honor your rights regarding what we collect, but it is your responsibility to contact the social media or website to exercise your data rights as allowed by local law.

- No Retaliation for Exercise of Privacy Rights

We will never retaliate against individuals exercising their choices or individual rights with respect to the processing of their Personal Information. That notwithstanding, failure to provide us with Personal Information or the authority to process it will prevent us in certain circumstances to provide certain Product or Services, or to include you in programs or activities. Subject to applicable Data Protection Laws, we may also offer different levels of pricing or goods or services depending on your choices to allow us to process certain types of Personal Information. We aim to alert you in case your choices with respect to the processing of Personal Information by us will impact our ability to provide Products or Services to you.

Additional Rights Available Under Local Law (GDPR, California)

In the event that Personal Information is collected or processed by an entity controlled by the Company subject to GDPR or UK GDPR or Swiss law, you have additional individual rights (Data

Subject Rights) to access and information with respect to Personal Information collected about you, and to control our use of such information. Details can be found on our GDPR Privacy page.

California residents who are consumers have specific rights with respect to Personal Information collected about them by businesses. Details can be found on our California Privacy Rights page.

11. CHILDREN'S PRIVACY

In general, our websites and online resources are not directed at children, and of the online services that we offer are designed for individuals who are 18 years of age or older. Where requests for information about a medication are permitted by law, individuals requesting information about a medication, even if indicated for use in children, must be 18 years of age or older unless otherwise permitted by law.

We do not knowingly collect Personal Information from children under 13 years of age, or according to local law, without obtaining verifiable parental consent prior to collection. If you are a parent or guardian and believe we have collected information from your child, please contact the Global Privacy Office to request removal at privacyoffice@organon.com.

From time to time, some of our websites and other online resources may provide optional features for children. When we do offer those features, we will take appropriate steps to ensure that verifiable parental consent is obtained prior to any collection, use or disclosure of Personal Information from children.

12. QUESTIONS AND COMPLAINTS

If you have any questions or concerns about our Privacy Practices, please feel free to reach out to us using the contact information set out in the next paragraph. If we process your Personal Information, you have the right to complain about how we handle your Personal Information if you are concerned that we do not follow our policies or fail to respect your privacy rights.

Who to Contact with your Privacy Concerns and Complaints?

If you reside in an EEA country, please contact the Company's EU Data Protection Officer by e-mail at euprivacydpo@organon.com.

If you are residing in the U.S. or any other country outside the EEA, please contact our Global Privacy Office by email to: privacyoffice@organon.com or by postal mail to: Chief Privacy Officer, Organon & Co., 30 Hudson Street, Jersey City, NJ 07302.

Employees and contractors are required to promptly inform the Global Privacy Office or the designated Business Practice Manager for their business area of any questions, complaints or concerns related to our Company's Privacy Practices.

How we Process any Inquiries and Complaints

We will review and investigate all questions, complaints or concerns related to our Privacy Practices, whether received directly from employees or other individuals or through third parties,

including, but not limited to accountability agent, regulatory agencies, and other government authorities. If you are contacting us to access, correct or to cause us to delete Personal Information or to exercise any other rights that you may have under applicable Data Protection Laws as a data subject or consumer, we are required to verify that the requestor is authorized to make such a request. Typically, we are attempting to match the name and/or email used in connection with your request with information in our records and systems. Depending on the nature of your request and additional requirements established by local law, we may need to validate additional data points to reach the legally required degree of certainty to act on your request. We aim to provide a written response within forty-five (45) days from the receipt of your communication, or earlier if required as a matter of law. We will update you if we are unable to complete our response within forty-five (45) days, and if required by applicable Data Protection Laws, provide you with further information, such as the reasons for the delay and when we expect to complete our response, or why we are unable to complete your request and whether you have any further options to appeal our decision. We may extend the original forty-five (45) day response period by up to additional forty-five (45) days.

Right to Complain with Supervisory Authorities or to Seek Legal Redress

If the processing of your Personal Information by us was subject to GDPR, you have specific rights to seek governmental redress.

You may lodge a complaint with the locally competent Supervisory Authority if you believe that our Privacy Practices or the handling of your compliant violated your rights as a data subject under GDPR. A list of the respective agencies acting as Supervisory Authorities and their addresses can be found here: Our Members | European Data Protection Board (europa.eu).

You may also bring an action to enforce your data subject rights in the courts of the EEA country (i) where you reside or (ii) where the entity responsible for the processing activity giving rise to your compliant has its establishment for GDPR purposes. For the avoidance of doubt, nothing herein shall operate as a consent to general or special jurisdiction by any Organon entity other than specifically required by Art. 79 GDPR.

Your right to lodge a complaint or to sue is also available to you if you seek to enforce your rights as third party beneficiary in connection with the transfer of your Personal Information by way of Standard Contract Clauses.

13. MISCELLANEOUS, UPDATES

We reserve the right to modify, add, or remove portions of this notice at any time by publishing an updated notice on our website at https://organon.com/privacy. Any changes will become effective at the time of publication unless otherwise stated.

14. GDPR PRIVACY RIGHTS

GDPR establishes a heightened standard of accountability for parties determining the means and purposes of any given operation involving the processing of Personal Information or processing Personal Information on their behalf. Among other things, GDPR prohibits the processing of

Personal Information without specific legal authority (legal basis). Following is an overview of the legal bases commonly relied upon by us.

Legal Basis Authorizing Processing of Personal Information

- Consent

  Our businesses subject to GDPR rely on the consent of data subjects in most cases when we engage directly with individuals, for example to collect their contact information or to reach out for marketing activities, such as the sending of promotional materials. Consent may be expressed explicitly, for example by ticking a box or by other means that signals to us clearly that the individual intends to allow us to process Personal Information. We will strive to make it clear whenever we ask for your consent and document your consent in our records.

  You may withdraw your consent at any time by contacting the privacy office responsible for your country of residence. Our processing of your Personal Information before you inform us about the withdrawal of our consent is not affected by that withdrawal.

  Consent for processing of sensitive data, such as health-related data, must be specific and explicit. We will endeavor to clearly communicate the nature of our request if we ask you to consent to processing of sensitive data.

- Fulfillment of Contracts

  GDPR authorizes us to process Personal Information to the extent necessary to prepare or to fulfill a contract with you or with a third party which we are entering into at your request. Typical cases involve our dealings with suppliers and contractors but also the processing of certain Personal Information in our function as employer, e.g., when we process Personal Information to pay salaries or administer benefits.

- Compliance with Legal Obligations

  In many instances, various laws and regulations, such as tax regulations or immigration or social security laws, require us to process Personal Information on an ongoing basis. We may also be required to report certain events regarding the efficacy or safety of our Products or Services to regulatory entities. We may also be compelled to disclose Personal Information to governmental authorities and third parties in the context of investigations and legal process.

- Legitimate Interests

  In many instances, we rely on the authorization to process Personal Information to pursue the legitimate interests of the Company, for example when we develop and grow our business or market our Products or Services. We use this legal basis for processing Personal Information also if it is impractical or impermissible to obtain your consent and no

other legal authority for processing of Personal Information is available. In each case, we conduct an analysis to ensure that privacy interests of the affected individuals are protected. Whenever we rely on our legitimate interests as grounds for processing you have special rights as a data subject outlined below. We will never process sensitive information, such as health-related data, on the basis of legitimate interests.

- Other Legal Bases

  The above is merely an overview featuring the most common legal bases relied on by us. In particular in the area of scientific research and employment law, national laws of individual Member States of the EU offer additional statutory authorizations for processing Personal Information.

Individual Rights (Data Subject Rights)

- Procedural Rights

  In addition to the choices for Customers to access and control the use of their Personal Information GDPR provides individuals with specific rights in connection with their Personal Information, known as Data Subject Rights. If you believe that we are processing any Personal Information about you - regardless of whether you are a Customer or not – you may exercise the rights described below by using this form or the forms on our local contact page available in the languages of the EEA countries where we do business.

  We will respond to your request within a month after we received your request, either by completing your request or explaining why we need more time or may be unable to complete your request in part or as a whole. We may extend the response time for up to two additional months. As a part of our response process, we will need to verify that you are the individual whose Personal Information is the subject matter of your request.

- Additional Information and Access Rights

  You have the right to know:

  - the sources of Personal Information about you collected from third parties; and,
  - the categories of third parties your Personal Information was shared with;
  - whether or not your Personal Information was used for automated decision-making including profiling; and,
  - whether your Personal Information was transferred to a recipient in a country outside the EEA that has not yet been found to have a GDPR equivalent level of data protection. In that case we will inform you about our measures to protect your exported Personal Information.
  - You have the right to inspect copies of the instruments (SCCs or other data transfer documents) we rely on to govern the export of Personal Information to

recipients in Third Countries. We will redact any such copies to the extent their disclosure may jeopardize the rights of other parties or our interest to protect proprietary or confidential information or trade secrets.

- Right of Correction

  In addition to the choices available to any Customer, we will honor all requests to correct or to, if so warranted, supplement your Personal Information that is incorrect or out of date.

- Right of Erasure

  You have the right to direct us to delete any Personal Information about you that we are processing. In certain instances, we are authorized to refuse such request, for example, if the data in question continue to be needed for the lawful purposes for which they were collected or if deleting such data would infringe on certain rights of other parties.

- Right to Restrict Processing

  In certain instances, for example while we are investigating your claim that we are processing incorrect information about you, or if we are processing Personal Information on the basis of our pursuit of legitimate interests and you objected to such processing, we will restrict such processing at your request until we have completed our investigation.

- Right to Data Portability

  Upon your request we will provide you with the data sets comprising the Personal Information about that we are processing in a machine-readable structured format to facilitate its transfer to another party designated by you.

- Right to Object to Further Processing

  In specific cases, you have the right to object against our otherwise lawful processing of Personal Information about you, if you believe that your personal circumstances are such that resulting potential harm outweighs our legitimate interests in processing your information. Those include:

  - ❖ Processing of Personal Information based on the pursuit of legitimate interests; or,

  - ❖ Processing Personal Information about you for scientific, historical, or statistical purposes in reliance on a statutory provision authorizing us to do so without your consent or any other legal basis

  In those instances, we will halt our processing activities until we have determined, whether we are able to safeguard you interests through additional measures to protect you and inform you about our findings before resuming our processing activities.

- Right to Object to Use of Personal Information for Direct Marketing

If your Personal Information is used by us for direct marketing, you may direct us at any time to stop the use of your information for that purpose, including any profiling in connection with such marketing activities.

- Rights in Connection with Automated Decision Making

  We will not make decisions based solely on automated decision making that have significant impact on you unless it is necessary for the entering into or the performance of a contract with you, or when you have given your specific consent.

  In order to protect you in case we make a decision based solely on automated processing of your Personal Information which produces legal or other significant effects on you, you have the right: to obtain human intervention, to express your point of view, to obtain an explanation of the decision reached after an assessment, and to challenge such a decision.

15. GLOSSARY OF PRIVACY TERMS

Anonymization
The alteration, truncation, obliteration or other redaction or modification of Personal Information to render it irreversibly incapable of being used to identify, locate, or contact an individual, either alone or in combination with other information.

Company
Organon & Co., its successors, subsidiaries, and divisions worldwide, excluding joint ventures to which our Company is a party.

Deidentification
The removal of direct and indirect personal identifiers, often preserving the original identification data separately.

Applicable Law
All applicable laws, rules, regulations, and orders of opinions having the force of law in any country in which our Company operates or in which Personal Information is processed by or on behalf of our Company. This includes all privacy frameworks under which our company has been approved or certified including the Asia Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPRs").

Personal Information
Any data relating to an identified or identifiable individual, including data that identifies an individual or that could be used to identify, locate, track, or contact an individual. Personal Information includes both directly identifiable information such as a name, identification number or unique job title, and indirectly identifiable information such as date of birth, unique mobile or wearable device identifier, telephone number as well as key-coded data, online identifiers such as IP addresses or any personal activities, behavior, or preferences which may be collected to provide services or products.

Privacy Incident
A violation of this Policy or a privacy or data protection law and includes a Security Incident. Determinations of whether a privacy incident has occurred and whether it should be elevated to a Personal Data Breach shall be made by the Global Privacy Office, Business Technology Risk Management (BTRM), and Legal.

Processing
Performing any operation or set of operations on information about people, whether or not by automatic means, including, but not limited to, collecting, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, evaluation, analysis, reporting, sharing, disclosure, dissemination, transmission, making available, alignment, combination, blocking, deleting, erasure or destruction.

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information, or our Company's reasonable belief of the same. Access to Personal Information by or on behalf of our Company without the intent to violate this Policy does not constitute a Personal Data Breach, providing that the Personal Information accessed is further used and disclosed solely as permitted by this Policy.

Security Incident
An information security incident is made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations.

Sensitive Information
Any type of information about people that carries an inherent risk of potential harm to individuals, including information defined by law as sensitive, including, but not limited to information related to health, genetics, biometrics, race, ethnic origin, religion, political or philosophical opinions or beliefs, criminal history, precise geo-location information, bank or other financial account numbers, government-issued identification numbers, children who are minors, sex life, sexual orientation, trade union affiliation, insurance, social security and other employer or government-issued benefits.