Policy Number: 13.2.1
Policy Title: Global Cross Border Privacy Rules
Policy Type: Internal and Publicly Facing at www.msd.com/privacy/cross-border-policy
Version: 1.3
Effective Date: 30 April 2018

Global Cross Border Privacy Rules Policy

At Merck & Co., Inc. (Kenilworth, NJ, USA), which is known as MSD outside of the U.S. and Canada, our mission of saving and improving lives extends to respecting privacy and protecting personal information.

We strive to conduct our business in accordance with our privacy values because we believe they demonstrate our unwavering commitment to ethical and responsible practices. We recognize that innovation and new technology drive continual change in risks, expectations and laws, so we follow privacy accountability standards and aim to promptly adapt how we apply them in response to those changes.

This Policy defines our global standards for management and protection of Personal Information by or on behalf of our company that directly or indirectly originates from any country in the European Economic Area ("EEA"), Switzerland or from Asia Pacific Economic Cooperation ("APEC") member economies and is transferred to any other country, including transfers between the EEA and APEC. It describes our core commitments supporting compliance with our APEC Cross-Border Privacy Rules certification, our Binding Corporate Rules ("BCRs"), which have been approved in the European Union, and our self-certification to the EU-U.S. Privacy Shield. It applies to our operations in every country, to every activity involving information about people that we conduct in every subsidiary and every division (including by any successors to our business), including, but not limited to our research, manufacturing, commercial, corporate support activities and healthcare services and solutions and the data transfers necessary to carry out those activities, including, but not limited to:

- Research and Manufacturing: evaluating needs and opportunities for medical and health innovation; initiating, managing and financing research studies; evaluating and engaging researchers, scientific and ethics committee members and business partners to support our research studies and the development of our products; research study recruitment; evaluating the safety, efficacy and quality of our investigational and marketed products; meeting our product safety and product quality obligations, including handling and reporting adverse events and product quality complaints; filing for approval and registering our products with health regulatory authorities; and complying with associated legal, regulatory or ethical requirements;
- Commercial: evaluating the markets for our products; advertising, marketing, selling, distributing and delivering our products; communicating and engaging with health care professional customers, health care payers, patients and other end users of our products, as well as caregivers of those who use our products; sponsoring and conducting events; evaluating and engaging business partners to support our commercial activities; and complying with associated legal, regulatory or ethical requirements;
- Corporate Support: recruiting, hiring, managing, developing, communicating with, and compensating employees; administering benefits for employees and their dependents; conducting employee performance and talent reviews; providing training and other learning and development programs; conducting employee disciplinary and grievance proceedings; managing ethics and privacy concerns and conducting investigations; managing and securing our physical and virtual assets and infrastructure; procuring and

Pr Proprietary

paying for goods and services; meeting our environmental, health and safety and other corporate responsibility commitments; engaging with the media; and complying with associated legal, regulatory or ethical requirements.

- Healthcare Services and Solutions: improving the value of care delivered to patients worldwide through evidence-based services and solutions focused on clinical services, engagement solutions and health analytics.

This Policy also applies to all people about whom we process information, including, but not limited to, our health care professional and other customers; prospective, current and former employees and their dependents, patients, caregivers, researchers and research study participants, scientific and ethics committee members, business partners, investors and shareholders, government officials, and other stakeholders.

All Company Employees and Senior Leaders have core privacy responsibilities they must uphold.

We recognize that inadvertent errors and misjudgments related to protection of information about people can create privacy risks for individuals and reputational, operational, financial and compliance risks for our Company. We will provide appropriate training on this Policy to all employees and other personnel who have permanent or regular access to Personal Information, who are involved in the collection of data or in the development of tools used to process Personal Information. Every employee of our company, and others who process information about people for our company, is accountable for understanding and upholding their obligations under this Policy and applicable Laws.

Our Privacy Values and Standards

We uphold our privacy values in everything we do involving people including how we apply our privacy standards. Our four privacy values are:

Respect	Trust	Prevent Harm	Comply
We recognize that privacy concerns often relate to the essence of who we are, how we view the world and how we define ourselves, so we strive to respect the perspectives and interests of individuals and communities and to be fair and transparent in how we use and share information about them.	We know that trust is vital to our success, so we strive to build and preserve the trust of our customers, employees, patients and other stakeholders in how we respect privacy and protect information about people.	We understand that misuse of information about people can create both tangible and intangible harms for individuals, so we seek to prevent physical, financial, reputational and other types of privacy harms to individuals.	We have learned that laws and regulations cannot always keep pace with the rapid change in technologies, data flows, and associated shifts in privacy risks and expectations, so we strive to comply with both the spirit and letter of privacy and data protection laws and regulations in a manner that drives consistency and operating efficiency for our global business operations.

1. We embed our privacy standards into all activities, processes, technologies and relationships with third parties that use Personal Information. We **design privacy controls into our processes and technologies that are consistent with our privacy values and standards and applicable law**. Our 8 privacy principles set forth below summarize our privacy standards and core requirements for processes, activities and their supporting technologies at a high level.

Pr Proprietary

Privacy Principle	Our Core Commitments
1. **Necessity** – Prior to collecting, using, or sharing Personal Information, we define and document the specific, legitimate business purposes for which it is needed.	• We determine and document how long Personal Information is needed for those defined business purposes and applicable legal requirements. • We do not collect, use or share 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 the data when business requirements necessitate that information about the activity or process is 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.
2. **Fairness** – We don't process Personal Information in ways that are unfair to the people to whom those data relate.	• We determine whether the proposed collection, use or other processing of Personal Information presents a likely and/or severe risk of tangible or intangible harm to individuals in accordance with our privacy value to *Prevent Harm*. • If the nature of the data, types of people, or the activity present a likely and/or severe risk of tangible or intangible harm to individuals, we ensure that the risk of harm is outweighed by a corresponding benefit to those individuals or to our mission of saving and improving lives, and mitigated by the measures, safeguards and mechanisms we have put in place. • Where the risk appears to outweigh the benefits to individuals, we only process the Sensitive Information or Personal Information with the explicit consent of the individuals, as expressly required or expressly permitted by applicable law, or as expressly authorized by a competent regulatory authority. • We document the risk analysis and design any required mechanisms to obtain and document evidence of consent into supporting technologies.
3. **Transparency** – We don't process Personal Information in ways or for purposes that are not transparent.	• All individuals about whom Personal Information is processed under this Policy shall have a right to a copy of this Policy. We will make copies of this Policy available online at www.msd.com/privacy. The Merck Global Privacy Office will provide electronic and/or paper copies of this Policy upon request to the addresses listed in Section 3.a. below. • ***When Personal Information is collected directly from individuals***, we inform them, prior to collecting the information and through a clear, conspicuous, and easily accessible privacy notice or similar means, of (1) the company entity or entities responsible for the processing, (2) the contact details of our Chief Privacy Officer and/or the regional/local Data Privacy Officer, (3) what information will be collected, (4) the purposes for which it will be used, (5) the legal basis for our processing, (6) with whom it will be shared, including any requirements to disclose Personal Information in response to lawful requests by government authorities, (7) whether and how we will transfer the Personal Information to other countries, including the relevant countries where feasible (8) how long it will be retained or the criteria by which we make that determination, (9) how they can ask a question, raise a concern or exercise their rights related to their Personal Information, (10) how they can withdraw any consent they have provided, (11) their right to lodge a complaint with a supervisory authority, (12) any obligation to provide Personal Information and the consequences of not doing so, (13) any automated decision-making, including

Pr Proprietary

	profiling, we will carry out, and (14) a link to this Policy, where possible and appropriate. Our comprehensive privacy notices for many of our stakeholders are available online at http://www.msd.com/about/how-we-operate/privacy/transparency-and-privacy.html • *When Personal Information is obtained through observation, sensors, or other indirect means*, it may not be possible to provide a privacy notice directly to the individual at the time the information are collected. In such cases, we assure transparency to the individual through other means, such as posted or printed on the device or materials associated with the device that will obtain the information. • *When Personal Information is collected by way of a web site, mobile app, or other online application or resource*, we apply the technology-specific standards set forth in our Internet Privacy Policy and our Cookie Privacy Commitment to ensure the requirements for being transparent in accordance with this Policy have been met. • *When Personal Information is collected from other sources and not specifically at the direction of our company*, prior to obtaining the information, we verify in writing that the provider of the information has informed individuals of the ways and purposes for which our company intends to use the information. If written verification cannot be obtained from the provider of the information, we use only anonymized information, or prior to using Personal Information, we inform the affected individuals through a privacy notice or similar means of (1) the entity or entities of our company responsible for processing the information, (2) the contact details of our Chief Privacy Officer and/or the regional/local Data Privacy Officer, (3) what information our company plans to use, (4) the purposes for which our company plans to use it, (5) the legal basis for our processing, (6) with whom our company will share it, (7) whether and how we will transfer the Personal Information to other countries, including the relevant countries where feasible (8) how long our company plans to retain it or the criteria by which we make that determination, (9) how they can ask a question, raise a concern or exercise their rights related to their Personal Information, (10) how they can withdraw any consent they have provided, (11) their right to lodge a complaint with a supervisory authority, (12) any obligation to provide Personal Information and the consequences of not doing so, (13) any automated decision-making, including profiling, we will carry out, and (14) a link to this Policy, where possible and appropriate. • We ensure that the necessary transparency mechanisms, including, where possible, mechanisms that support individual rights requests, are designed into supporting technologies, and that third parties supporting the activity or process do not process information about people in ways that are inconsistent with what individuals have been told through a privacy notice or other verifiable means that we and others working for us will do with the information.
4. **Purpose Limitation** –We only use Personal Information in accordance with the Necessity and Transparency principles.	• If new legitimate business purposes are identified for Personal Information that previously was collected, 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, including materially similar to, purposes described in a privacy notice or other transparency mechanism that was previously provided to the individual. We will determine compatibility based on (1) any link between the original purposes and the proposed new purpose, (2) the reasonable expectations of the individual, (3) the nature of the Personal Information, (4) the consequences of the further processing for the individual, and (5) the safeguards we have put in place.

Pr Proprietary

	• We do not apply this principle to anonymized information or where we use Personal Information solely for historical and scientific research purposes and (1) 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, (2) we have put in place appropriate safeguards to ensure data minimization, such as pseudonymization, and (3) all other applicable Laws are respected. • We ensure that purpose limitation restrictions are designed into any supporting technology, including any reporting capabilities and downstream data sharing.
5. **Data Quality** – We keep 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. • Where changes are made to Personal Information by our company or third parties working for our company, we ensure that those changes are communicated to the relevant individuals in a timely manner where reasonably possible.
6. **Security** – We implement safeguards to protect Personal Information and Sensitive Information from loss, misuse, and unauthorized access, disclosure, alteration or destruction.	• We have implemented a comprehensive information security program and we apply security controls that are based on the sensitivity of the information and the risk level of the activity, taking into account current technology best practices and the cost of implementation. 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.
7. **Data Transfer** – We are responsible for and we preserve the privacy protections for Personal Information when it is transferred to or from other organizations or across country borders.	(1) We transfer Personal Information within our company if the following requirements are met: (1) the sharing is necessary to fulfil the purpose for which the Personal Information was originally collected or another legitimate interest of the company, and (2) the purpose for which it is to be shared, and the fact that it will be shared, is consistent with the privacy notice or other transparency mechanism that was previously provided to the individual at the time the Personal Information was originally collected and the individual gave their consent where necessary. (3) where one of our company subsidiaries acts solely on behalf of another of our company subsidiaries in processing Personal Information, (4) where required by Law, those subsidiaries of our company will execute an internal data processing agreement in accordance with Principle 8 of this Policy. (2) We only transfer Personal Information to or allow it to be processed by third parties if the following requirements are met and we are liable for ensuring that the third parties we engage meet these requirements: • *If the role of the third party is to process Personal Information for or on behalf of our company*, before providing Personal Information to the third party or engaging the third party, we: (1) complete privacy due diligence to evaluate the privacy practices and risks associated with those third parties, (2) obtain contractual assurances from those third parties that they will process Personal

Pr Proprietary

Information pursuant only to our company's instructions, and in accordance with this Policy, including without limitation all 8 Privacy Principles and the other standards set forth in this Policy, and applicable Laws, that they will notify our company promptly of any Privacy Incident, including any inability to comply with standards set forth in this Policy and applicable Laws, or Security Incident, and cooperate to promptly remediate any substantiated Incident and to address the individual rights set forth in Section 2 below, that they will not engage another company to process the Personal Information without our written authorization and without putting in place an agreement imposing equivalent data protection obligations, that they will delete or return to us all Personal Information after they have finished providing services to us or upon our request, and that they will permit our company to audit and monitor their practices for the duration of the processing for compliance with these requirements. Additionally, if the third party processes Personal Information that originates in a country or territory with a law that restricts the transfer of Personal Information, we will ensure that the transfer to the third party meets the requirements for cross-border data transfer described in (3) below.

- *If the role of the third party is to supply Personal Information to our company,* before obtaining Personal Information from the third party, we ensure that the Transparency requirements for collecting Personal Information from other sources and not specifically at the direction of our company are met, and we obtain contractual representations from the third party that it is not violating any Law or the rights of any third party by providing Personal Information to our company.
- *If the role of the third party is to receive information from our company for processing that is not specifically at the direction of our company,* before providing information to the third party, we ensure that the information has been anonymized, and we obtain written assurances from the third party that they will use it only for business purposes defined in the agreement and in accordance with applicable laws, and that they will not attempt to re-identify the information.
- *If the transfer to a third party is required to protect the individual's legitimate interests or those of the company,* we may transfer the information: (1) for the purposes of fraud prevention or to enforce or protect the rights and properties of the company, (2) for the protection of the personal safety of our employees or third parties on our property, and (3) to protect our assets by taking corrective security measures if we reasonably suspect that unlawful activity or serious misconduct has taken place.
- *If the third party is a target for acquisition or a controlling interest by our company*, (1) prior to entering into an agreement to acquire the third party or to acquire a controlling interest in the third party, we complete privacy due diligence to evaluate the privacy practices and risks associated with acquisition of that third party or a controlling interest in that third party, and (2) we enter into a data transfer agreement that specifies the terms and conditions under which Personal Information may be disclosed and the respective obligations of our company and the third party.
- *If the role of the third party is to acquire all or part of our company's business*, prior to sharing any Personal Information in connection with a divesture of any part of our company's business, we (1) enter into a data transfer agreement that specifies the terms and conditions under which Personal Information may be

Pr Proprietary

	disclosed to the purchaser, including appropriate limitations as to the permitted uses of the Personal Information and compliance with the standard set forth this Policy and applicable Law, (2) review all data elements about people prior to sharing to evaluate the requirements for sharing, (3) obtain consent to share Personal Information or Sensitive Information in accordance with the Transparency and Purpose Limitation principles of this Policy, and (4) require the third party to notify our company promptly of any applicable Privacy Incident, including any inability to comply with standards set forth in this Policy and applicable Laws, and cooperate to promptly remediate any substantiated Incident or cease Processing relevant Personal Information. (3) We transfer Personal Information across country borders, including to the United States of America, by or on behalf of our company in accordance with this Policy. We will apply this Policy to transfers of Personal Information from any other country or territory with a law that restricts the transfer of Personal Information, in addition to complying with any requirements imposed by such Laws (including the use of any mechanisms required for cross-border transfers).
8. **Legally Permissible** – We only process Personal Information if the requirements of applicable laws have been met.	• While the other 7 privacy principles, as well as the Individual Rights requirements described below, are intended to ensure that the requirements of most privacy and data protection laws that apply to our business around the world have been met, in some countries, we need to meet additional requirements, including but not limited to the following: 1) Where required, we will obtain specific forms of consent for certain processing of Personal Information, including but not limited to, approval of the processing by works councils and other labor unions; 2) Where required, we will register processing of Personal Information with or seek the approval of the applicable privacy or data protection regulatory authority; 3) Where required, we will provide broader rights (for example, of access and correction) than set forth in this Policy; 4) Where required, we will further limit data retention periods for Personal Information; and 5) Where required, we will enter into agreements containing specific contractual clauses, including agreements for cross-border data transfer to third parties. 6) Where required, we will disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. In the event of a conflict between this Policy and an applicable law, the standard that provides more protection to individuals will prevail.

2. <u>We will promptly address individual rights requests to access, amend, correct or delete Personal Information, to object to the processing of Personal Information about them, or to exercise other rights regarding their Personal Information</u>.
   a. **Access, Correction, Deletion, and other rights** – Under Laws in most countries in which we operate, individuals have a right to access Personal Information about themselves, and to amend, correct or delete Personal Information that is inaccurate, incomplete or outdated. We will honor all requests to

Pr Proprietary

access, correct and delete Personal Information from all individuals in accordance with Section 3a below. If a request for access, correction or deletion is governed by an applicable Law that provides greater protection to individuals, we will ensure that the additional requirements of that Law are met. In some countries, individuals may be entitled to other rights with respect to Personal Information about themselves, such as a right to restrict processing, to object to processing (see also Section 2b below), and to have their data transferred to another service provider. We will honor the exercise of data rights in accordance with applicable Laws.

b. Choice – Consistent with our privacy values of "Respect" and "Trust," we honor individual requests to object to Personal Information processing, including, but not limited to opting out of programs or activities in which they previously agreed to participate, processing of Personal Information about them for direct marketing communications, communications targeted to them based on Personal Information about them, and any evaluation of or decisions about them, which has the potential to significantly affect them, made by use of automation or algorithms.

    i. Except where prohibited by Law, we may deny the choice where a particular choice request would impede our company in its ability to: (1) 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, (2) investigate, make or defend legal claims, and (3) perform contracts, administer relationships, or engage in other permitted business activities that are consistent with the Transparency and Purpose Limitation principles and were entered into in reliance on the information about people in question. Within fifteen business days of any decision to deny a choice request in accordance with this Policy, we will document and communicate the decision to the requestor.

3. We will promptly respond to and escalate all privacy-related questions, complaints, concerns and any potential Privacy Incident or Security Incident.

    a. Any individual about whom we processes Personal Information within the scope of this Policy can raise a question, complaint or concern to our company at any time, including a request for a list of all subsidiaries of our company that are subject to this Policy. We expect that our employees, and others who work on behalf of our company, provide prompt notice if they have a reason to believe that an applicable Law may prevent them from complying with this Policy. Any question, complaint or concern raised by an Individual, or any notice provided by an employee or any other person who works on behalf of our company, should be directed to the Merck Global Privacy Office:

        i. By e-mail to: msd_privacy_office@msd.com

        ii. By postal mail to: Privacy Office, Merck & Co., Inc., UG4B-24, 351 N. Sumneytown Pike, North Wales, Pennsylvania, USA 19454.

    b. Employees and contractors are required to promptly inform the Merck Global Privacy Office, or the designated Privacy Steward for their business area, of any questions, complaints or concerns related to our company's privacy practices.

    c. The Merck Global Privacy Office will review and investigate, or will work with the Office of Ethics, Legal and/or Compliance, to investigate, all questions, complaints or concerns related to our company's privacy practices, whether received directly from employees or other individuals or through third parties,

Pr Proprietary

including, but not limited to regulatory agencies, accountability agents and other government authorities. We will respond to the individual or entity that raised the question, complaint or concern to our company within thirty (30) calendar days unless a Law or the third party requestor requires a response in a shorter period of time or unless circumstances, such as a concurrent government investigation, require a longer time period, in which case the individual or third party requestor will be notified in writing as soon as practicable of the general nature of the circumstances contributing to the delay.

d. The Merck Global Privacy Office, in coordination with Legal and Compliance, will cooperate in response to any inquiry, inspection or investigation of a privacy regulatory authority.

e. For complaints that cannot be resolved between our company and the individual who raised the complaint, our company has agreed to participate in the following dispute resolution procedures in the investigation and resolution of complaints to resolve disputes pursuant to this Policy, however, at any time, individuals resident in the EEA or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA, may also rely on standard 3.f. below:

   i. for disputes involving all Personal Information received by our company from Switzerland, our company has agreed to cooperate with the Swiss FDPIC;

   ii. for disputes involving the transfer to the U.S. of Personal Information related to human resources activities and collected in the context of an employment relationship in the EEA, our company also commits to cooperate with the appropriate EU data protection authority panel.

   iii. for disputes involving all other Personal Information under this Policy, including, but not limited to those involving our company's compliance with the Asia Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPRs"), the EU-U.S. and Swiss-US Privacy Shield, our company has agreed to dispute resolution by TRUSTe, a U.S.-based dispute resolution provider. Individuals who submit a question or concern to our company and who do not receive acknowledgment from our company of the inquiry or who think their question or concern has not been satisfactorily addressed should then contact the TRUSTe Dispute Resolution Program on the Internet, by mail or by fax. Inquiries by mail or fax should identify Merck & Co., Inc. or MSD as the company to which a concern or question has been submitted, and include a description of the privacy concern, the name of the individual submitting the inquiry, and whether TRUSTe may share the details of the inquiry with our company. TRUSTe will act as a liaison to our company to resolve these disputes.
      1. Online
      2. Fax: +1-415-520-3420
      3. Mail: Watchdog Complaints, TRUSTe, 835 Market Street, Suite 800, Box 137 San Francisco, CA, USA 94103-1905

   iv. For information about TRUSTe or the operation of TRUSTe's dispute resolution process, visit TRUSTe on the Internet or request this information from TRUSTe by mail or fax using the contact information listed above. The TRUSTe dispute resolution process shall be conducted in English.

Pr Proprietary

v. For any dispute arising under the EU-U.S. and Swiss-US Privacy Shield that is not resolved through the steps described in this section, individuals have the option to invoke binding arbitration in accordance with the procedures for the Privacy Shield Panel set up under the EU-U.S../.Swiss-U.S. Privacy Shield.

f. All individuals residing in the EEA, or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA, about whom information is processed pursuant to this Policy have the right under this Policy, at any time, to enforce the requirements of this Policy as third party beneficiaries, including the right to bring a judicial action to seek remedies for breach of his or her rights under this Policy (as set out in Section 2, above) and the right to receive an award for damages resulting from such breach. Individuals residing in the EEA or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA (for the sake of clarity, including to the USA), may bring a claim or a complaint under this Policy, against Merck, Sharp & Dohme (Europe) Inc. -Belgium Branch ("MSD Europe"):
   i. In the courts or with the data protection authority in the EEA country from which Personal Information about them was transferred,
   ii. In the courts or with the data protection authority in the EEA country of their habitual residence, or
   iii. In the courts of Belgium or with the Belgian Privacy Commission.

g. Our company will respond to the individual or entity that raised the question, complaint or concern to our company within thirty (30) calendar days unless a Law or the third party requestor requires a response in a shorter period of time or unless circumstances require a longer time period, in which case the individual or third party requestor will be notified in writing.

4. We are accountable for upholding our privacy values and standards.
   a. The subsidiary of our company accountable for an action that gives rise to a substantiated Privacy Incident or Security Incident is financially responsible for the amount of any claim for damages or fine or penalty arising out of the Privacy Incident or Security Incident.
      i. In coordination with and at the direction of the Merck Global Privacy Office, MSD Europe is responsible for ensuring that the necessary actions are taken to address any alleged violations of this Policy by subsidiaries of our company outside of the EEA affecting individuals residing in the EEA or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA, and, where required, to pay the fines, penalties or damages awarded for violations of this Policy affecting individuals residing in the EEA or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA. With support from the Merck Global Privacy Office and the subsidiary of our company outside of the EEA accountable for the alleged violation, MSD Europe shall be responsible for demonstrating that our company is not liable for the alleged violation. Where another subsidiary of our company is accountable for the action that necessitated the fine, penalty or award of damages, such subsidiary may be required to promptly reimburse MSD Europe for any amount paid by MSD Europe. If a subsidiary of our company outside the EEA breaches this Policy, the courts or the data protection authorities in the EEA will have jurisdiction and the

Pr Proprietary

affected individual will have the rights and remedies against MSD Europe as set out in Section 3.f. above.

ii. In coordination with and at the direction of the Merck Global Privacy Office, **Merck Sharp & Dohme Corp.** is responsible for ensuring that the necessary actions are taken to address any alleged violations of this Policy affecting individuals residing outside of the EEA and, where required, to pay the fines, penalties or damages awarded for violations of this Policy affecting individuals residing outside of the EEA or individuals about whom Personal Information is not subject to the data protection Law of the EEA. Where another subsidiary of our company is accountable for the action that necessitated the fine, penalty or award of damages, such subsidiary may be required to promptly reimburse Merck Sharp & Dohme Corp. for any amount paid by Merck Sharp & Dohme Corp.

Oversight and Monitoring

In order to provide assurance to regulators and other stakeholders that our company is accountable for its commitment to ethical and responsible privacy practices, the company maintains an extensive oversight and monitoring governance group, headed by a **Chief Privacy Officer** with a dedicated Global **Privacy Office (GPO), an assigned EU DPO, Country DPO's where required by law or local authorities,** and **Privacy Stewards**, who are appointed by Senior Leaders and serve as liaisons between the Merck Global Privacy Office and the organizational areas in which they work.

Our company will rely on the **Privacy Accountability Agents** to whom it is responsible under Laws to periodically verify its compliance with the requirements of this Policy and those Laws, including the APEC CPBRs.

In addition to the assurance reviews managed by the Merck Global Privacy Office, internal and external audit and assurance teams will conduct compliance reviews to verify that Merck is adhering to this Policy, including any policies, procedures, standards and guidance subordinate to this Policy. Corrective and preventative action plans will be developed and implemented to address gaps observed by the audit and assurance teams. The results of the Audit Program will be communicated to the Chief Privacy Officer and the Privacy and Data Protection Board, who are responsible for reporting them as described in this Policy.

Privacy and Data Protection Authorities who have approved this Policy or who have jurisdiction over our company's practices under this Policy have a right to verify our compliance with it. We will abide by the advice of these competent authorities with respect to the interpretation and application of this Policy.

Terms You Need to Know

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

Pr Proprietary

Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPRs"), the EU-US and Swiss-US Privacy Shield - under the investigatory and enforcement powers of U.S. Federal Trade Commission.

- **Our company.** Merck & Co., Inc. (Kenilworth, NJ, USA), its successors, subsidiaries and divisions worldwide, excluding joint ventures to which our company is a party.
- **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 and online identifiers such as IP addresses.
- **Privacy Incident.** A violation or breach 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 is material shall be made by the Merck Global Privacy Office, Information Technology Risk Management and Security (ITRMS), and the Office of General Counsel.
- **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.
- **Security Incident.** 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 Security Incident, provide that the Personal Information accessed is further used and disclosed solely as permitted by this Policy.
- **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.
- **Third party**. Any legal entity, association or person that is not owned by our company, or in which our company does not have a controlling interest, or who is not employed by our company. Except as expressly set forth in this Policy, no subsidiary or division of our company shall be required to meet the requirements of a third party under this policy as all subsidiaries or divisions are required to process information about people in accordance with this Policy, including in circumstances where one of our company subsidiaries supports one or more other subsidiaries of our company in the processing.

Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of applicable Law. A notice will be posted on our company's privacy web page (www.msd.com/privacy) for 60 days whenever this Policy is changed in a material way.

Effective Date

Pr Proprietary

Pr Proprietary