Second Sight Medical Products, Inc. Privacy Policy for US-EU Privacy Shield

Effective Date: March 1, 2018

Second Sight Medical Products, Inc. and its Swiss subsidiary, Second Sight Medical Products (Switzerland) Sàrl, (collectively "SSMP") have adopted this Privacy Shield Policy ("Policy") to establish and maintain an adequate level of Personal Information privacy protection. This Policy applies to the processing of Personal Information that SSMP obtains from Individuals located in the European Economic Area, directly or through Switzerland.

SSMP complies with the EU-U.S. Privacy Shield Framework, as set forth by the U.S. Department of Commerce, regarding the collection, use, and retention of Personal Information transferred from the European Economic Area to the United States. SSMP has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. All SSMP employees who handle Personal Information from the European Economic Area are required to comply with the Principles stated in this Policy. If there is any conflict between the terms in this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall prevail. To learn more about the Privacy Shield program, and to view SSMP's certification, please visit https://www.privacyshield.gov/.

This Policy outlines SSMP's general policy and practices for implementing the Privacy Shield program as described below.

For purposes of this Policy:

"Individual" shall mean any natural person who is located in the European Economic Area, The term also shall include any individual agent, representative, of an individual and all employees of SSMP residing in the EEA, where SSMP has obtained his or her Personal Information from such Individual as part of its business relationship with SSMP.

"Data Subject" shall mean an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics. For those residing in Switzerland, a Data Subject also may include a legal entity.

"EEA" shall mean the European Economic Area.

"Employee" shall mean an employee (whether temporary, permanent, part-time, or contract), former employee, independent contractor, or job applicant of SSMP or any of its affiliates or subsidiaries, who is also a resident of a country within the EEA.

"Personal Information" shall mean any information, including Sensitive Personal Information, that (i) is transferred to SSMP in the United States from the EEA, directly or through Switzerland, pursuant to the Privacy Shield programs, (ii) is recorded in any form, (iii) relates to an identified or identifiable Individual, and (iv) can be linked to that Individual. For

Switzerland, the term "person" includes both a natural person and a legal entity, regardless of the form of the legal entity.
"Sensitive Personal Information" shall mean Personal Information about racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health or medical records, sex life, or criminal records.

"Third Party" shall mean any individual or entity that is neither SSMP nor an SSMP employee, agent, contractor, or representative.

"Privacy Shield" shall mean the US-EU Privacy Shield Framework, a program of the US Department of Commerce.

"Privacy Framework" refers to the Privacy Shield Framework, a program of the US Department of Commerce.

Scope

This Policy applies to the processing of Individual Personal Information that SSMP receives in the United States concerning Individuals who reside in the EEA, directly or through Switzerland. This Policy does not cover data from which individual persons cannot be identified, or situations in which pseudonyms are used since the use of pseudonyms involves the replacement of names or other identifiers with substitutes so that identification of individual persons is not possible.

Responsibilities and Management

SSMP has designated the Legal Department to oversee its information security programs, including its compliance with the EU and Swiss Privacy Shield program. The Legal Department shall review and approve any material changes to this program as necessary. Any questions, concerns, or comments regarding this Policy should be directed to privacy@secondsight.com.

SSMP will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Information that it collects. SSMP personnel will receive training, as applicable, to effectively implement this Policy.

Renewal/Verification

SSMP will renew its US-EU Privacy Shield and Swiss-US Privacy Shield certifications annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, SSMP will conduct an in-house verification to ensure that its attestations and assertions about its treatment of Individual Personal Information are accurate and that SSMP has appropriately implemented these practices. Specifically, as part of the verification process, SSMP will undertake the following:

- review this Policy, and its publicly posted website privacy policy, to ensure that these policies accurately describe the practices regarding the collection of Individual Personal Information;
- ensure that the publicly posted privacy policy informs Data Subjects of SSMP's participation in the US EU Privacy Shield and US Swiss Privacy Shield programs and where to obtain a copy of additional information (e.g., a copy of this Policy);
- ensure that this Policy continues to comply with the Privacy Shield Principles;
- confirm that Individuals are made aware of the process for addressing complaints and any independent dispute resolution process (SSMP may do so through its publicly posted website);
- review its processes and procedures for training employees about SSMP's participation in the Privacy Shield programs and the appropriate handling of Individual's Personal Information; and
- will prepare an internal verification statement on an annual basis.

Collection and Use of Personal Information

SSMP complies with the Privacy Shield Framework regarding the collection, use, and retention of Personal Information transferred from EEA, directly or through Switzerland, to the U.S. pertaining to:

- clinical research site staff, such as Investigators and Health Care Professionals;
- potential and active clinical research participants and patients (data used for clinical or scientific research and other related purposes should be anonymized when appropriate);
- human resources, such as candidates, residing in the EEA (SSMP maintains an internal policy that addresses the compliance with the Privacy Shield Principles for employees)
- business partners and/or customers, residing in the EEA;
- vendors, consultants and/or suppliers, residing in the EEA; and
- investors, residing in the EEA.

Scope and Purpose of Processing of Personal Information

SSMP collects, retains and processes personal information for the following reasons:

- data processor for the purposes of clinical research activities, clinical research management, clinical research support, statistical analysis of clinical studies, regulatory affairs, and services to customers based on agreements executed between parties;
- data controller for the purposes of recruiting and maintaining potential and current clinical research participants, investigators, and facilities;
- data controller for the purposes of safety and efficiency monitoring, data analytics purpose, customer relationship management, customer service, marketing and advertising, and community outreach;
- data controller for the purposes of recruiting personnel and administering and carrying out the employment or personnel relationship.

Disclosures/Onward Transfers of Personal Information

Except as otherwise provided herein, SSMP discloses Personal Information only as required by law and to Third Parties who reasonably need to know such data and only for the scope of the initial purpose. All Third Parties must agree to abide by confidentiality obligations.

SSMP may provide Personal Information to Third Parties that act as agents, consultants, and contractors to perform tasks on behalf of and under SSMP's instructions. For example, SSMP may store such Personal Information in the facilities operated by Third Parties. Such Third Parties must agree to use such Personal Information only for the purposes for which they have been engaged by SSMP, and they must also either:

- comply with the Privacy Shield principles or another mechanism permitted by the applicable EU & Swiss data protection law(s) for transfers and processing of Personal Information; or
- agree to provide adequate protections for the Personal Information that are no less protective than those set out in this Policy.

SSMP also may disclose Personal Information for other purposes, or to other Third Parties, when a Data Subject has consented to or requested such disclosure. It should be noted that SSMP may be required to disclose an Individual's Personal Information in response to a lawful request by public authorities, including for product safety or efficacy monitoring activities. This includes reports from healthcare providers, reports to government agencies, and as may be required by law. SSMP will be liable for appropriate onward transfers of Personal Information to Third Parties.

Sensitive Personal Information

For sensitive information, SSMP will obtain express consent, or an opt-in selection, from individuals if such information is to be:

- disclosed to a third party; or
- used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals by indicting the opt-in choice.

In addition, when the third party identifies and treats the Personal Information as sensitive, SSMP will also treat the Personal Information that was received from a third party as sensitive.

Data Integrity and Security

SSMP uses reasonable efforts to maintain the accuracy and integrity of Personal Information and to update it as appropriate. SSMP has implemented physical and technical safeguards to protect Personal Information from loss, misuse, unauthorized access, disclosure, alternation, or destruction. For example, electronically stored Personal Information is stored on a secure network with firewall protection, and access to SSMP's electronic information systems requires user authentication via a log in and password or similar means. Remote access is through a VPN

with two step authentication. SSMP also employs access restrictions, limiting the scope of employees who have access to Individual Personal Information.

Further, SSMP uses secure encryption technology to protect certain categories of Personal Information, such as email messages and portable devices. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

Notification

SSMP notifies Individuals about its adherence to the EU-US Privacy Shield and Swiss-US Privacy Shield principles through its privacy policy that is publicly posted on its website at http://www.secondsight.com. SSMP also takes into account individual consent and adherence to this Policy when Personal information is received.

Accessing Personal Information

SSMP Employees may access and use Personal Information only if they are authorized to do so and only for the purpose for which they are authorized.

Right to Access, Change, or Delete Personal Information

Right to Access. Data Subjects have the right to know what Personal Information about them is included in databases, and to ensure that such Personal Information is accurate and relevant for the purposes for which SSMP collected it. Data Subject's may review their own Personal Information stored in databases and correct, erase, or block any data that is incorrect, as permitted by applicable law and SSMP policies.

Right to Change. Upon reasonable request, and as required by the Privacy Shield principles, SSMP allows Data Subjects access to their Personal Information in order to correct or amend such data where inaccurate. Data Subjects may edit their Personal Information by contacting SSMP in writing at 12744 San Fernando Road, Suite 400, Sylmar, CA 91342, USA, Attn: Privacy Official, or by email at privacy@secondsight.com. In making modifications to their Personal Information, Data Subjects must provide only truthful, complete, and accurate information.

Right to Delete. To request deletion of Personal Information, Data Subject's should submit a written request to SSMP at 12744 San Fernando Road, Suite 400, Sylmar, CA 91342, Attn: Privacy Official. Data Subjects may decide or be asked to withdraw from a clinical trial at any time. Any Personal Information collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, as provided by notice to Data Subjects at the time of participation.

Requests for Personal Information. SSMP will track each of the these requests and will provide notice to the appropriate parties under law and contract, except if the request for disclosure of Personal Information is received by a regulatory or law enforcement authority or if prohibited by law or regulation.

Satisfying Requests for Access, Modifications, and Corrections. SSMP will respond in a timely manner, but no more than forty-five (45) days, to all reasonable written requests to view, modify, or inactivate Personal Information.

Changes to this Policy

This Policy may be amended from time-to-time, consistent with the Privacy Shield Principles and applicable data protection and privacy laws and principles. SSMP will make the public and employees aware of changes to this Policy either by posting on its website, http://www.secondsight.com/, through email messaging, or by similar means. SSMP will notify Individuals of any changes made that materially affect the way SSMP handles Personal Information that has been previously collected. SSMP will then allow Individuals to choose whether their Personal Information may be used in a materially different manner, such as for future scientific research.

Enforcement and Dispute Resolution

In compliance with the US-EU and Swiss-US Privacy Shield Principles, SSMP commits to resolve complaints regarding Individual's privacy and the collection or use of Personal Information. EEA Individuals with questions or concerns about the use of Personal Information should contact SSMP at privacy@secondsight.com.

If an Individual's question or concern cannot be satisfied through this process, SSMP has further committed to refer unresolved privacy complaints under US-EU Privacy Shield and Swiss-US Privacy Shield to an independent dispute resolution mechanism, at no cost to the Individual, operated by the American Arbitration Association.

If resolution to a complaint is not received within forty-five (45) days, or if the complaint is not satisfactorily addressed by SSMP, EEA Individuals may bring a complaint before the American Arbitration Association. American Arbitration Association's EU and Swiss Privacy Shield program can be found at: http://go.adr.org/privacyshield.html. Finally, as a last resort and in limited situations, EEA individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

SSMP will take steps to remedy any issues that arise out of a failure to comply with the relevant Privacy Frameworks principles.

SSMP commits to cooperate with EEA data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EEA in the context of the employment relationship.

Due Diligence and Audits

SSMP is a publically traded corporation, and as such is regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed publically

too prematurely. Similarly, if SSMP becomes involved in a potential merger or takeover, it will need to perform, or be the subject of, a "due diligence" review. This will often entail the collection and processing of Personal Information, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the Individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

Questions or Complaints

EEA Individuals can contact SSMP with questions or complaints concerning this Policy or SSMP's practices concerning Personal Information at the following address:

Second Sight Medical Products, Inc.
Attention: Privacy Official
12744 San Fernando Road
Suite 400
Sylmar, CA 91342
USA
Email: privacy@secondsight.com

Last Revised: March 1, 2018