STAAR Data Privacy Framework Addendum

Effective date: 17 April 2024

STAAR Surgical Company (“STAAR”, “we”, “us” and “our") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. STAAR has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. STAAR has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program and to view our certification, please visit **dataprivacyframework.gov/**.

Please see the **STAAR Privacy Policy** for more information on how STAAR conducts cross-border transfers of personal data and the measures we take to safeguard personal data in accordance with applicable legal requirements. STAAR is subject to the authority of the Federal Trade Commission.

This Addendum outlines our general policy and practices for implementing the EU-U.S. DPF Program (refers collectively to the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF), including the types of personal data processed by STAAR and for which the Program is applicable; how we use it; and the choices that affected individuals have regarding our use of, and their ability to correct, the personal data relating to them. If there is any conflict between this Addendum and the Principles, the Principles will govern. To learn more about the EU-U.S. DPF Program and to view STAAR’s certification, please visit **dataprivacyframework.gov/s/participant-search**.

This Addendum applies to personal data that we handle. For purposes of this statement, “personal data” means information that:

- Is transferred from the European Economic Area (EEA), Switzerland and/or the United Kingdom to the United States, in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF
- Is about, or pertains to, a specific individual
- Can be linked, either directly or indirectly, to that individual

Principles protecting individuals’ privacy notice and choice

- We notify individuals about the personal data that we collect from them, how we use it and how to contact us with privacy concerns.
- We provide such notice through this Addendum, our Privacy Policy or other similar documents, and direct communication with individuals from whom we collect personal data.

- We collect and process personal data about STAAR personnel for the purpose of human resources administration and recruitment following the EU-U.S. DPF Program.
- We collect and process personal data about our prospective and current customers and/or customer personnel and patients for the purpose of rendering professional services to our customers.
- We collect and process personal data from individuals who use STAAR's websites, service platforms, mobile applications and other properties.
- We collect personal data from individuals only as permitted by the EU-U.S. DPF Program.
- Consent for personal data to be collected, used and/or disclosed in certain ways (including opt-in consent for sensitive data) may be required in order for an individual to obtain or use our services. Such consent is provided through our customer acknowledgments; email, platform and website notices; and other similar mechanisms.

Disclosures and transfers

We do not disclose an individual's personal data to third parties, except when one or more of the following conditions is true:

- We have the individual's permission to make the disclosure.
- The disclosure is required by lawful request by public authorities, including to meet national security or law enforcement requirements.
- The disclosure is required by law or mandatory professional standards.
- The disclosure is reasonably related to the sale or other disposition of all or part of our business.
- The information in question is publicly available.
- The disclosure is reasonably necessary for the establishment of legal claims.
- The disclosure is to another STAAR entity or to persons or entities providing services on our or the individual's behalf (each a transferee), consistent with the purpose for which the information was obtained, if the transferee, with respect to the information in question:
    - Is subject to law providing an adequate level of privacy protection
    - Has agreed to provide an adequate level of privacy protection

We may transfer personal data from one jurisdiction to another. Privacy laws vary by jurisdiction, and some may provide less or different legal protection from others. However, STAAR will protect personal data in accordance with the EU-U.S. DPF Program regardless of the jurisdiction in which the data resides.

STAAR is responsible for the third-party acts within its control that result in the processing of personal data inconsistent with the EU-U.S. DPF Program.

Data, security, integrity and access

We employ various physical, electronic and managerial measures, including education and training of our personnel, that are designed to reasonably protect personal data from loss, misuse or unauthorized access, disclosure, alteration or destruction. Personal data collected or displayed through a website is protected in

transit by standard encryption processes. However, we cannot guarantee the security of information on, or transmitted via, the internet.

We process personal data for only the limited and specific purpose for which it was originally collected or authorized by the individual. To the extent necessary for such purposes, we take reasonable steps so that personal data is accurate, complete, current and otherwise reliable with regard to its intended use.

An individual has the right to access personal data that STAAR holds about that person as specified by the EU-U.S. DPF Program. An individual may also exercise other rights by providing detailed instruction to PrivacyOffice@staar.com to correct, amend or delete information where it is inaccurate or has been processed in violation of the Principles; or restrict or object to the processing or disclosure of personal data (in certain circumstances and subject to applicable law). The individual will need to provide sufficient identifying information, such as name, address, and birth date. We may request additional identifying information as a security precaution, such as a national identifier (e.g., a government issued ID or notarization).

We may limit or deny access to personal data where providing such access would be unreasonably burdensome or expensive in the circumstances or where the rights of persons other than the individual would be violated. In some circumstances, we may charge a reasonable fee for access to personal data.

Accountability and enforcement

We have established a program to monitor our adherence to the EU-U.S. DPF Program and to address questions and concerns regarding our adherence. This program will include a statement, at least once a year, signed by an authorized representative of STAAR, verifying that this statement is accurate, comprehensive for the information that is intended to be covered, prominently displayed, completely implemented and accessible. We encourage interested persons to raise any concerns with us using the contact information below.

Individuals may file a complaint with PrivacyOffice@staar.com in connection with STAAR's processing of their personal data under the EU-U.S. DPF Program. With respect to any dispute relating to this statement that cannot be resolved through our internal processes, unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF may be made to the **International Centre for Dispute Resolution - American Arbitration Association (ICDR)**, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit the ICDR website (https://www.icdr.org/dpf) for more information or to file a complaint. The services of the ICDR are provided at no cost to you.

Personnel who violate our privacy policies will be subject to disciplinary process.

An individual may, under certain conditions, invoke binding arbitration. Please see the **EU-U.S. DPF website** for more information on conditions giving rise to binding arbitration.

Amendments to this Addendum

We may amend this Addendum from time to time by posting a revised statement on this website or a similar website that replaces this website. If we amend the Addendum, the new notice will apply to personal data previously collected only insofar as the rights of the individual affected are not reduced. So long as we adhere to the EU-U.S. DPF Program, we will not amend our Privacy Policy and DPF Addendum in a manner inconsistent with the EU-U.S. DPF Program.

Information subject to other policies

We are committed to following the Principles for all personal data within the scope of the EU-U.S. DPF Program. However, certain information is subject to policies of the firm that may differ in some respects from the general policies set forth in this Addendum. STAAR websites, mobile applications and service platforms (collectively, "Sites") have their own Privacy Policy and Terms of Use that apply to those Sites. That Privacy Policy may be accessed here.

Information relating to present or former STAAR personnel is subject to our policies concerning personnel data privacy, which are available to current STAAR personnel on the STAAR intranet site and to former STAAR personnel upon request.

Contact information

For further information or to make a request or complaint, please contact us:

STAAR Privacy Office:

Kathleen Determann
STAAR Surgical Co.
25510 Commercecentre
Lake Forest, California 92630
USA
PrivacyOffice@staar.com

EU Data Representative:

STAAR Surgical AG
Niederlassung DE ("STAAR DE")
Harksheider Str. 3
22399 Hamburg, DE
DPRepresentative@staar.com

STAAR DE External DPO:

Dr. Sebastian Kraska
IITR Datenschutz GmbH
Eschnrieder Str. 62c
82194 Groebenzell, DE
Email@IITR.de