



CORPORATE POLICY: Global Privacy Policy

Valid from: February 2022

Owner: Head of Global Compliance & Data Privacy



A. GENERAL INFORMATION

Sonova AG is incorporated under the laws of Switzerland, as a data controller, with its registered address at Laubisrütistrasse 28, 8712 Stäfa, Switzerland, and operates with its affiliates located around the world (collectively referred to as the “Company” or “we” or “our”).

As the Company processes Personal Data in its day-to-day business, this Global Privacy Policy (“Policy”) has been drafted and implemented in order to describe the Company’s practices regarding the use of Personal Data about its customers, contractors and partners (“Data Subjects”). The Company pays particular attention to the respect of privacy and Personal Data and is committed to complying with this Policy, in accordance with applicable local laws.

By “Personal Data” we mean any information relating to an identified or identifiable natural person.

By “processing” we mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

B. POLICY’S APPLICABLE LAW

The Company undertakes to comply with the applicable data protection law (“Applicable Law”). Thus, depending on the countries where the Company is established, the processing of Personal Data will be subject to the local Applicable Law. Although certain requirements may vary from one country to another, the Company is particularly concerned about the privacy of Data Subjects, and this Policy constitutes a global guideline to which the Company is committed.

In particular, the Company is committed to complying with the following laws, where applicable:

- The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement



CORPORATE POLICY: Global Privacy Policy

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (“GDPR”). The GDPR aims to harmonize and frame the rules relating to the processing of Personal Data on the territory of the European Union in order to provide a single legal framework for professionals, and seeks to strengthen control by citizens of the use that may be made of Personal Data concerning them. This regulation, applies to the processing of Personal Data for UE citizens or residents and for the activity of a controller or a processor in the UE territory.

- The Swiss law Federal Act on Data Protection of June 19, 1992 (“FADP”), modified in 2020 in order to adapt to current technological and align with the GDPR and other recent European regulations.
- The California Consumer Privacy Act of 2018 (“CCPA”) which aims to provide more transparency and to guarantee more rights to consumers residing in California whose Personal Data are processed by companies.
- The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) which defines the United States rules for the electronic processing of health data by health actors and business partners.

C. PERSONAL DATA COLLECTED

The Company may process the following Personal Data:

- Identity data: last name, first name, nationality and date of birth
- Contact details data: postal address, private phone number, private email address and emergency contact
- Social security reference number and insurance company
- Financial data: means of payment, financial institution, IBAN
- Data relating to the user health : weight, height, medical trouble, doctor’s prescription, hearing capacity, physical activity tracking (step count, exercise intensity, exercise minutes), fitness data (heart rate, energy expenditure, blood pressure)
- Data relating to the user behavior on the website
- Data relating to the product purchased by the customer: model, serial number, usage data
- Data relating to the service provided
- Data relating to the feedback the customer provides on our products and services: comments and notes

In addition, as our activity is mainly focused on manufacturing innovative solutions for hearing aids, we may be required to collect sensitive Personal Data and more specifically health data. Depending on the country where the Data Subject reside, those sensitive Personal Data may benefit from special protection, particularly in terms of security and confidentiality measures implemented.

D. PURPOSES OF PROCESSING PERSONAL DATA

The following legal bases constitute the foundation on which the Company relies to carry out the processing of Personal Data. Other legal bases may be used depending on where the Data Subject resides and the relevant Applicable Law.

Some processing of Personal Data may be based on the consent of Data Subjects. The processing of Personal Data for this purpose may involve:

- Marketing purposes such as sending newsletters and information about products and services offered by the Company
- To improve the performance of our website



CORPORATE POLICY: Global Privacy Policy

- To advise and interact with you : for the creation of your account, to contact us via the contact form, for Sonova to respond to users, to take an online hearing test

The processing of Personal Data that the Company carries out may also be based on the execution of a contract or pre-contractual measures with Data Subjects. The processing of Personal Data for this purpose may involve:

- Fulfillment of our contractual obligations towards Data Subjects
- Provision of after-sales service after the purchase of a product by a customer
- Social Security / insurance processing
- Claims management

The Company may also process Personal Data based on its legitimate interest, in particular in order to improve our products and services, customer experience and internal processes. The processing of Personal Data for this purpose may involve:

- Conducting statistical/usage analysis
- Performing internal administrative functions
- Processing customer requests
- Prevent fraudulent activity and improve security
- Relationship management with Data Subjects
- Evaluation of the relevance of our products and services

The Company may also process Personal Data in order to respond to legal requirements. Processing based on legal requirement depends on the Applicable law.

E. RETENTION OF PERSONAL DATA

Personal Data will not be kept longer than necessary for the above-mentioned purposes. This means that Personal Data will be deleted as soon as the purpose of the processing of Personal Data has been achieved. However, the Company may retain Personal Data longer if necessary to comply with Applicable Law, or if necessary to protect or exercise our rights, to the extent permitted by applicable data protection law.

At the end of the retention period, the Company may also need to archive Personal Data, to comply with Applicable Law, for a limited period of time and with limited access.

These retention periods may vary depending on the country where the Data Subjects reside and in accordance with Applicable Law.

F. DISCLOSURE OF PERSONAL DATA

The Company may share Personal Data, subject to your consent or other relevant legal basis, with the following third-parties:

- Other companies of our group such as subsidiaries and affiliated companies
- Trusted business partners providing services on our behalf, such as for technical support, for marketing purposes or for other types of service delivery
- Governmental authorities and public authorities, as far as this is necessary to provide any services that have been requested or authorized, to protect customers, contractor and partners' rights, or our or others' rights, property or safety, to maintain the security of our services or if we are required to do so because



CORPORATE POLICY: Global Privacy Policy

of Applicable Law, court or other governmental regulations, or if such disclosure is otherwise necessary in support of any legal or criminal investigation or legal proceeding

Depending on Applicable Law, we implement contracts with some third-parties to ensure that Personal Data are processed based on our instructions and in compliance with this Policy and any other appropriate confidentiality and security measures.

G. TRANSFERS OF PERSONAL DATA

The above-mentioned third-parties such as affiliates and subsidiaries, as well as business partners, public authorities to whom we may disclose Personal Data, may be located outside of a Data Subject's country of domicile, potentially including countries whose data protection laws may differ from those in the country in which Data Subjects are located.

If Personal Data are processed within the European Union/European Economic Area, and in the event Personal Data are disclosed to third parties in a country not considered as providing an adequate level of protection according to the European Commission, the Company will ensure:

- The implementation of adequate procedures to comply with Applicable Law, and in particular when a request for authorization from the competent supervisory authority is necessary
- The implementation of appropriate organizational, technical and legal safeguards to govern the said transfer and to ensure the necessary and adequate level of protection under Applicable Law
- If necessary, the implementation of Standard Contractual Clauses as adopted by the European Commission
- If necessary, take supplementary measures such as completing a data transfer adequacy assessment if, after evaluation of the circumstances of the transfer, and after evaluation of the legislation of the third country, it is necessary for the protection of the transferred Personal Data.

If Personal Data are not processed within the European Union/European Economic Area, and in the event Personal Data are disclosed to third parties located outside the Data Subject's jurisdiction, the Company will ensure that appropriate safeguards are in place to protect Personal Data by implementing appropriate legal mechanisms. Those mechanisms may differ depending on the country and relevant Applicable Law.

H. PERSONAL DATA SECURITY

The Company implements a variety of security measures, according to Applicable Law, in order to protect Personal Data from security incidents or unauthorized disclosure, and more generally from a Personal Data breach. These security measures are recognized as appropriate security standards in the industry and include, inter alia, access controls, password, encryption and regular security assessments.

If a Personal Data breach occurs, and in particular if there is a breach of security resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise processed, the Company will take appropriate measures such as:

- Investigating and analyzing in order to determine the consequences of the Personal Data Breach and in particular whether it is likely to create a risk for the rights and freedoms of those affected
- If the analysis shows that there is a risk to the rights and freedoms of those affected, the Company will notify the competent authority and, in case of high risk, communicate to those affected
- Implement as soon as possible the measures necessary to remediate and mitigate the Personal Data breach
- Document the Personal Data breach in order to ensure its traceability

Appropriate measures and procedures in the event of a Personal Data breach may differ depending on the country where it occurs, the type of breach and depending on the relevant Applicable Law.



CORPORATE POLICY: Global Privacy Policy

I. PRIVACY RIGHTS RELATED TO PERSONAL DATA

As may vary based on relevant Applicable Law, Data Subjects have rights related to their Personal Data, such as the right to request access, rectification, erasure of their Personal Data, restriction of processing, object to processing, request data portability, to be informed and withdraw their consent for processing of Personal Data based on their consent. Data Subjects may also object to automated individual decision-making if they are concerned by such processing.

In addition, in some jurisdictions you may provide instructions relating to the retention, communication and erasure of your Personal Data posthumously.

The exercise of such rights is not absolute and is subject to the limitations provided by Applicable Law.

Data Subjects may have the right to lodge a complaint with the local supervisory authority or the competent regulator if they consider that the processing of their Personal Data infringes Applicable Law.

To exercise those privacy rights, Data Subjects may contact us as described in the section “How to contact us” below. We may ask proof of identity in order to respond to the request. If we can’t satisfy your request (refusal or limitation), we will motivate our decision in writing.

J. UPDATES TO THIS POLICY

If necessary, we may from time to time need to update this Policy in order to reflect new or different privacy practices. In this case, we will post updated versions of this Policy on this page. A revised Policy will apply only to data collected subsequent to its effective date. We encourage you to periodically review this page for the latest information on our privacy practices.

K. HOW TO CONTACT US

For any questions, comments, or concerns about this Policy, or in order to exercise the privacy rights permitted by Applicable Law related to Personal Data, please contact our Data Protection Officer at the following address: Sonova AG, Laubisruetistrasse 28, 8712 Stäfa, Switzerland or by sending an e-mail at: privacy@sonova.com