30. SEPTEMBER 2021

# Privacy Policy

**Introduction**

The use of our website (iccortho.org or any subdomain) is possible without disclosure of personal data. However, if you want to use features or become a Member of the ICCO, processing of personal data could become necessary. When necessary and in the absence of statutory basis for processing of personal data, we generally obtain your consent.

**Information Collected**

When you visit our website, we will store: the website from which you visited us from, the parts of our website you visit, the date and duration of your visit, your anonymized IP address, information about the device (device type, operating system, screen resolution, language, country you are located in, provider information, and web browser type) you used during your visit, and more (user ID, tracking cookies IDs, order IDs, time in local user's timezone, files that were clicked and downloaded, links to external websites that were clicked, pages generation time, random unique visitor ID, time of first visit, time of the previous visit, number of visits, mouse movements, clicks, and scrolls, form interactions, video and audio interactions, site searches, key words from search engines, custom dimensions and variables based on your account information etc.). We process this usage data for statistical purposes, to improve our site and services, to provide individual technical support and to recognize and stop any misuse. If you contact us through our website, we will keep a record of our correspondence.

**Network Accounts**

We collect the following information (membership registration data) from users to register them as Members (full accounts with ICCO membership): title, first name, last name, email, primary address, university/company/private practice, department, clinic, phone number, preferred language. When registering, users must provide a password.

Additional information may be collected for specific roles in the system and to provide the corresponding services: middle name, date of birth, gender, billing address incl. VAT number, practice/business address, additional phone numbers, public profile (public profile e-mail, public profile web link, public profile phone number, CV text visible on public profile), information about Study Club memberships, degree/name on ICCO membership certificate, ICCO roles & functions, anonymized credit card for automatic renewal, post nominals (e.g. DDS, DMD), PubMed ID, education, specialty, friends, professional affiliations, accessed learning items, transactions, vouchers, CPD/CME credit hours, medals, badges, events, messages and tasks, speaker profile (topic focus and language proficiency).

**Diagnostic and Clinical Data**

All diagnostic and clinical data (e.g. texts, images, videos) uploaded or submitted to our website by website users are voluntary and shall not include personal information relating to patients that is not anonymous, unless documented informed consent has previously been obtained from the patient (any recipient of health care services).

HOW WE USE INFORMATION

**Network Accounts**
The ICCO uses registration data to register interested individuals as Members, to administer our website and provide users with services through the ICCO. Registration data is also used to contact users by email with newsletters and service-related announcements. We may use registration data to contact users about products and services that we think may be of interest to them, to request user participation in surveys or other activities related to our website/projects with which we are involved.

**Diagnostic and Clinical Data**
Users control the purpose for which their diagnostic and clinical data is used on our website. We store diagnostic and clinical data, and personal information relating to patients on behalf of users, however we will not use them for our own purposes or make them available to anyone without informed consent.

**Information shared with Third Parties**
We may share the data of users with third parties in that we may use third-party suppliers (processors) to host and process data on our behalf, e.g. to host our website and to maintain our IT-systems. We will ensure that adequate security measures are in place to safeguard users' data and that applicable laws and regulations regarding data privacy are observed. We may also share your personal data with our legal entities and partners such as the local MIKRONA entity or the MIKRONA distributor active in the country of your domicile for purposes consistent with this privacy policy (e.g. to provide service or membership-related benefits) based on legitimate interest grounds or – in respect of Marketing purposes – with your consent. Under certain circumstances, we may be required to disclose your personal information in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

**Information Security**
We implemented numerous technical and organizational measures to ensure the most comprehensive protection of personal data processed through this website. However, Internet-based data transmissions may in principle have security gaps, so absolute protection may not be guaranteed. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of user information at any time. Among other practices, your account is protected by a password for your privacy and security. You must prevent unauthorized access to your account and personal information by selecting and protecting your password appropriately and limiting access to your computer or device and browser by signing off after you have finished accessing your account. In case of a personal data breach we will notify our supervisory authority and the users affected by that breach. For more serious breaches you will also be notified.

## COOKIES AND WEBSITE TRACKING

**Cookies**
Cookies are small files that are sent to your computer's hard drive using your web browser or other programs. These are stored locally on your computer and kept ready for later retrieval. We use cookies to enhance our services. Session cookies are only used for the session. These cookies are deleted after the session has ended, e.g. after leaving our website or closing the browser window. Other cookies remain on your device for a longer period and allow us to recognize your browser on your next visit.

**Google Analytics**
We may collect analytics data, or use third-party analytics tools such as Google Analytics, to help us measure traffic and usage trends for the service and to understand more about the demographics of our users. You can learn more about Google's practices at https://policies.google.com/privacy/partners, and view its currently available opt-out options at https://tools.google.com/dlpage/gaoptout.

**Social Plug-Ins**
We utilize social plug-ins (e.g. LinkedIn, Twitter, YouTube). If you are logged in on such a platform when using our website, these plug-ins collect information about you and associate them with your account. If such a transmission of information is not desirable for you, then you may prevent this by logging off from your social media accounts before using our website.

---

## YOUR PRIVACY RIGHTS

**Cookies**
Cookies can be accepted through our cookie banner or by adjusting your web browser settings. You can set your browser to notify you when cookies are being enabled or to reject cookies altogether. However, when you reject cookies, you may not be able to use all our website features.

**Marketing Communications**
You can opt-out of receiving promotional or marketing communications from us at any time, by using the unsubscribe link in the email or by changing the preferences in your account settings (restriction of processing). If you have any account for our services, we may still send you non-promotional, transactional communication e.g. service or membership-related emails.

**Data Subject Rights**
We regularly review and erase or anonymize stored personal data when we no longer need it. If you would like to access, review, update, rectify, and delete any personal information we hold about you, or exercise any other data subject right available to you, you can use our contact form.

Please note that we may still use any aggregated and pseudonymized personal information that does not identify any individual and may also retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

**International Data Transfer**
Personal information you submit on our website or through our services is sent to Switzerland and will be primarily processed by us in Switzerland and potentially in other countries, on our servers or on our hosted service providers' cloud servers on our behalf. These countries may not have similar data protection laws to those in your country of residence. However, we will always protect your information in accordance with this Privacy Policy wherever it is processed.

For your convenience, hyperlinks may be posted on our website that link to other websites. We are not responsible for, and this Privacy Policy does not apply to, the privacy practices of any other websites or of any companies that we do not own or control. Other websites may collect information in addition to that which we collect on our website. We do not endorse any of these other websites, the services or products described or offered on such other websites, or any of the content contained on the other websites. We encourage you to seek out and read the privacy policy of each other website that you visit to understand how the information that is collected about you is used and protected.

---

CONTACT INFORMATION

**Controller Details**
Controller for the purposes of the General Data Protection Regulation (GDPR), other data protection laws applicable in Member states of the European Union and other provisions related to data protection is: ICCO, Fortunagasse 15, CH-8001 Zürich, Switzerland, +41 (0)79 893 2996, info@iccortho.org, www.iccortho.org

If you have any questions or concerns regarding our Privacy Policy, please use our contact form.

**Definitions**
The data protection declaration of the ICCO is based on the terms issued by the European legislator for the adoption of the General Data Protection Regulation (GDPR). Our data protection declaration should be legible and understandable for the general public, as well as our Guests, Affiliates, Members and Partners.

**Personal Data**
Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Diagnostic and Clinical Data**
Diagnostic and clinical data include any genetic or biometric data or data concerning health. Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person. This data gives unique information about the physiology or the health of that natural person and is determined from an analysis of a biological sample from the natural person in question. Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as (facial) images, voice recordings or fingerprints. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about his or her health status.

**Processing**
Processing is 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.

**Restriction of Processing**
Restriction of processing is the marking of stored personal data with the aim of limiting their processing in the future.

**Pseudonymization**
Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

**Controller**
Controller or controller responsible for the processing is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Processor**
Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Third Party**
Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

**Consent**
Consent of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Personal Data Breach**
Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Supervisory Authority**
Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 GDPR.

In Switzerland this is the Federal Data Protection and Information Commissioner (FDPIC). The FDPIC supervises federal and private bodies, advises and comments on the legal provisions on data protection and assists federal and cantonal authorities in the field of data protection. The FDPIC informs the public about its findings and recommendations and maintains and publishes the register for data files.

**Changes to Privacy Policy**
We may need to change this Privacy Policy from time to time. You will be notified of changes on our website and/or by e-mail when we are required to do so by applicable law. The last update of this Privacy Policy is indicated by the date.