CMX Privacy Policy

Medartis and its affiliates ("Medartis") take the protection of personal data very seriously and treat your personal data as confidential and in accordance with applicable laws and regulations, including, but not limited to, the EU General Data Protection Regulation (GDPR). The use of your personal data by Medartis is carried out in strict compliance with the provisions on data protection, in order for you to also feel safe with us in terms of data protection.

It is important to us that you know what personal data is collected when you visit our website or use our services and offers, and how we use such data afterwards. This privacy policy is intended to provide you with information on the scope and purpose of the collection and use of personal data on our website and to inform you on how your personal data is protected from manipulation, loss, destruction or improper use.

The introduction of new technologies and the further development of this website may result in changes to this privacy policy, we therefore recommend that you read this privacy policy regularly.

All technical terms used in this privacy policy shall have the meaning set forth in Art. 4 GDPR (e.g., "personal data" or "processing").

Responsible person
Medartis AG
Hochbergerstrasse 60E
4057 Basel Switzerland
Phone: +41 61 633 34 34
Fax: +41 61 633 34 00
Mail: info@medartis.com

EU representative
Medartis GmbH
Am Gansacker 10
79224 Umkirch
Deutschland
Telefon: +41 61 633 34 34
Fax: +41 61 633 34 00
Mail: info@medartis.com

Data Protection Officer
(Central Data Protection Officer Switzerland, EU and UK)
Medartis AG
Hochbergerstrasse 60E
4057 Basel
Telefon: +41 61 633 34 34
Mail: dataprotection@medartis.com

Storage period

We generally delete your personal data as soon as it is no longer needed for the purposes for which it was collected or otherwise processed.

If we have asked for your consent and you have given it, we will delete your personal data if you withdraw your consent and there is no other legal basis for the processing.

We will delete your personal data if you object to the processing and there are no overriding legitimate reasons for the processing.

If deletion of your personal data is not possible due to a legal obligation (statutory retention periods, etc.) or because such data is required in order to assert, exercise or defend legal rights or claims, we will restrict the processing of your personal data.

With regard to the data of registered users, this generally means that your data is stored as long as the registration exists. With regard to patient data that has been transferred to us by the client for the purpose of fulfilling an order, we are legally obliged under the provisions of the Regulation (EU) 2017 / 745 (Medical Device Regulation, MDR) to store data relating to non-implantable products for a period of at least ten years and data relating to implantable products for a period of at least fifteen years from the date of manufacture of the last product.
Medartis will delete such data as soon as it is no longer necessary to achieve the purpose for which it was collected and is no longer subject to a legal retention period, however, at the latest after twenty years since the date of manufacture of the last product. Please take note of the right to erasure.

Further information on the storage period can be found in the following sections.

Your rights as a data subject
You have the following rights with regard to your personal data:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object
- Right to data portability

You have the right, for any reasons that may arise from your particular situation, and at any time, to revoke your consent to the processing of your personal data which is carried out on the basis of Article 6 para. 1 lit. e or f GDPR. Your personal data will then no longer be processed unless there are legitimate reasons, worthy of protection, for the processing which override any interests, rights and freedoms, you may have, or the processing serves to assert, exercise or defend a legal right or claim. If we process your personal data in order to carry out direct marketing, you have the right to object to the processing of your personal data for the purpose of such advertising at any time. We will then no longer process your personal data for these purposes.

You have the right to revoke your consent to the processing of your personal data at any time if you have previously given such consent. The revocation of consent does not affect the lawfulness of any processing carried out on the basis of such consent prior to the revocation. In order to revoke your consent, please contact the data protection officer listed above using the contact options provided.

You have the right to issue a complaint to a supervisory authority about our processing of your personal data.

Provision of your personal data
Our web platform is used for the secure and confidential exchange of health and patient data (further detailed below). We need such data in order to be able to offer a patient specific and individual solution for a certain patient ("Service") upon medical prescription by the treating medical staff of a hospital or other medical institute. Such Service typically (but not only) consists of surgical planning, the manufacture and provision of medical tools or custom made bone plates and screws for surgical fixation and correction of deformities and fractures.

We process personal data in various ways in order to manage our business activities, improve our website, provide customer service and provide other products and services to our customers and potential customers. We do not share your personal data with unrelated third parties for their independent use except as permitted or required by law, or with your consent and only subject to confidentiality agreements. To the extent required or permitted by law, we may also collect, use and disclose personal information in connection with security or law enforcement investigations or in the course of cooperating with authorities or the fulfilment of legal requirements.

Medartis only processes your personal data if there is a legal basis for doing so.

You are generally not obliged to provide any personal data. If this should nevertheless be the case, we will point this out to you separately when collecting your personal data (for example by marking the respective fields as mandatory in input forms).

Failure to provide your personal data will regularly result in not processing your personal data for one of the purposes described below and you not being able to take advantage of an offer related to the respective processing.

The use of our web platform and services is intended for the following user groups and purposes:

User groups
- Medical staff: registration to use our web platform with name, qualification, employer, address, telephone number and e-mail address, and further information, if provided;

- Medartis employees who need to be involved in the provision of the Service and are in communication with the medical staff, as well as the administrators of the web platform: these categories of staff have full access to user data and in particular to patient data. These persons are known by name and bound to confidentiality. Their identity may be communicated externally based on justified and legitimate request. For all other employees of Medartis or its service providers, personal data are only accessible in anonymized form and via encrypted connections.

Purposes

- Registration as a user or guest user of the Medartis web platform, as defined in the CMX terms and conditions: Medartis processes personal data of registered users and guest users to be able to provide the Service, and to verify such users' authorization in advance;

- Contacting users: We use the user's name, address, email address or telephone number in order to respond to a request and to contact the user.

Depending on the country where the user is located, the contact details (name, title, job title, telephone number, email address, clinic) can be forwarded to our local subsidiary or distributor in order to ensure the provision of the requested service.

If we have asked for your consent and you have given it, the legal basis for the processing is Art. 6 para. 1 lit. a. GDPR.

You can revoke your consent at any time. The revocation of your consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.

To withdraw your consent, you can use the link provided for this purpose in the emails or contact us at the contact details provided above.

If the processing is necessary for the performance of a contract or for the implementation of pre-contractual measures based on your request, the legal basis for the processing is also Art. 6 para. 1 lit. b GDPR.

- Patient Data: we use patient and health data provided by medical staff only to provide the requested service, in particular to develop and manufacture patient specific custom implants, planning tools, software, surgical techniques or other devices related to the surgical fixation and correction of fractures and deformities.
Specific patient data may be used internally by Medartis in pseudonymised form for the purpose of research, study, development or training.

Within the above-mentioned purposes, data processing is carried out in accordance with the legal basis pursuant to Art. 9 GDPR, para.2, lit. J as well as Art. 89 GDPR.

In case that a local subsidiary or distributor needs to be involved to fulfil the order request, only the personal and sensitive data will be transferred for the specified purpose and in consideration of data minimisation.

Processing of Patient Data

Patient Data is processed in accordance with the respective requirements of the Medartis, subsidiaries and/or distributor on behalf of the customer for the purpose of product ordering, delivery and if applicable, invoicing, and in order to comply with all applicable regulatory and legal requirements.

In processing patient data on behalf of the Customer, Medartis agrees to comply with GDPR.

The physician / data transmitter acknowledges that Patient Data is "sensitive data" and that for the Processing of Patient Data all obligations and requirements for the Processing of special categories of personal data under the GDPR have to be taken into account.
The physician / data transmitter confirms that the patient has been informed of and expressly agreed to the processing of his or her patient data by Medartis in the form required by law. A form that complies with the legal requirements (incl. GDPR) is available for download at https://www.medartis.com/fileadmin/user_upload/cmx/faq/Medartis_-_Declaration_of_consent.pdf.
The physican / data transmitter is free to use another form that meets the legal requirements.

Medartis processes patient data on behalf of the physican / data transmitter for the above-mentioned purposes as data controller pursuant to Art. 9 lit. 2 a GDPR in order to comply with all applicable legal and regulatory requirements.
The legal basis for the processing also results from Art. 6 lit.1 a GDPR.
The data will only be stored as long as the purpose of use and your consent are valid.

If we have asked for your consent and you have given it, the legal basis for the processing is Art. 6 para. 1 lit. a GDPR. You can revoke your consent at any time. The revocation of your consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation. To revoke your consent, you can contact us at the contact details provided above.

In the event, that your consent has not been obtained, the legal basis for the processing of these categories of personal data is Art. 6 para. 1 lit. f GDPR and Art. 9 Abs. 2 lit. a GDPR. Our legitimate interest is the initiation and provision of our Service. If the processing is necessary for the fulfilment of a contract or for the implementation of pre contractual measures based on your request, the legal basis for the processing further is Art. 6 para. 1 lit. b GDPR.

Transfer of your personal data

Our web platform is hosted on the hardware and software infrastructure of Microsoft Azure, where all data are stored in encrypted form. Microsoft confirms by means of contractual provision that access to user data is restricted and that confidentiality is ensured. With the exception of contact data required for the two-factor authentication, which is carried out through global providers, user data of European customers is stored exclusively on servers located in Europe. Should such data be transferred to a third country, Microsoft confirms that the requirements of the GDPR are complied with.

The medical staff collects and provides Medartis with health and other data of patients, which is required for the performance of the Service. Typical patient data includes surname, first name, date of birth, diagnosis, description of the requested service and image data – typically computer tomography ("CT") data and/or X-rays. Such data is only processed if the attending physician confirms, when uploading the data, that the informed consent of the respective patient pursuant to applicable data protection laws has been obtained. Medartis and its employees that receive patient data are obliged to process and

safeguard patient data with the same level of confidentiality as the holders of professional secrecy. We process your personal and sensitive personal data with the appropriate care!

Hosting

Our web platform is hosted on the hardware and software infrastructure of Microsoft Azure, a service of Microsoft Corporation. Microsoft may have access to personal data that is processed in the context of the use of our online offer. For more information about Microsoft Azure, the scope of data processing and the technologies and processes involved in using the respective service, please refer to the further information about the services we use under the following links.

Microsoft Azure
Provider: In the European Economic Area (EEA) and Switzerland, Microsoft Ireland Operations Limited, Dublin is the data protection agent for Microsoft Corporation, United States of America.

Website:
https://azure.microsoft.com/de-de/overview/trusted-cloud/privacy/

Further Information & Privacy:
https://privacy.microsoft.com
https://www.microsoft.com/trust-center/privacy
https://www.privacyshield.gov/welcome

Guarantee: EU standard contractual clauses

Web server log files

We process personal data of you in order to be able to show you our online offer and to optimize the stability and security of our online offer. Certain information (e.g., requested element, URL, operating system, date and time of the request, browser type and version, IP address, protocol, amount of data transferred, user agent, referrer URL, time zone difference to Greenwich Mean Time (GMT) and/or HTTP status code) are stored in so-called log files (access log, error log, etc.).

If we have asked for your consent and you have given it, the legal basis for the processing is Art. 6 para. lit. a GDPR. If we have not asked for your consent, the legal basis for the processing is Art. 6 para. 1 lit. f GDPR. Our legitimate interest is the proper display of our online offer and optimizing the stability and security of our online offer.

Security

We take reasonable precautions to protect all personal data collected by us against unauthorised access and use, we regularly review security measures and conduct regular training and awareness-raising activities. However, you are responsible for keeping your login details and passwords confidential.

For security reasons and to protect the transmission of your personal data and other confidential content, we use encryption on our domain.

This can be recognized by the character sequence „https://" and the lock symbol in the browser's address bar.

Regarding the encryption of the web platform, the TLS (Transport Layer Security) standard is used, which guarantees an encrypted connection to the Internet.

Contact

If you contact us, we will process your personal data which you have provided to us in order to process your inquiry.

Contact form

We use your name, address, e-mail address, IP address and the information you provide in the contact form to process your request and contact you.

If we have asked for your consent and you have given it, the legal basis for the processing is Art. 6 para. 1 lit. a GDPR. If we have not asked for your consent, the legal basis for the processing is Art. 6 para. 1 lit. f GDPR. Our legitimate interest is to process your request.

If the processing is necessary to fulfil contractual obligations or to carry out pre-contractual measures based on your request, the legal basis for the processing further is Art. 6 para 1 lit. b GDPR.

We do not use external online services to provide and maintain our e-mail boxes.

In this context, only the Microsoft Exchange application is used, which is operated by Medartis. The data is stored in our data centre in Switzerland.

Cookies & similar technologies

We use Cookies and similar technologies on our web platform. Cookies are text information that are stored on your terminal device. A distinction is made between session cookies, which are deleted immediately after you close your browser, and permanent cookies, which are only deleted after a certain period of time.

The following statements on cookies also apply to similar technologies, and to further processing in connection with cookies and similar technologies (analysis & marketing, etc.). This also applies in particular to any consent you may have given for the use of cookies. Such consent also applies to the use of similar technologies and the further processing in connection with cookies and similar technologies.

Cookies may be used to enable the use of certain functions. Cookies may also be used to measure the reach of our online offer, to design it according to needs and interests and thus to optimise our online offer and marketing. Cookies may be used by us and by external services.

We only use essential cookies. For cookie details, please see the Cookie Consent Tool that we use, if you reach us via the Medartis website.

Please also note the general privacy notice on the Medartis website. If we have asked for your consent and you have given such consent, the legal basis for the use of cookies according to this section is Art. 6 para. 1 lit. a GDPR. If we have not asked you for your consent, the legal basis for the processing is Art. 6 para. 1 lit. f GDPR. Our legitimate interest is the management of the used cookies and the related consents. Depending on the purpose of the processing, our respective legitimate interests are specified in the following sections.

If you have reached our website directly via cmx.medartis.com, please note the following cookie information.

We use cookies for the following application:
Our user authentication is based on Microsoft Azure B2C identity and access management. This system requires cookies to maintain the user session after login.

Without these cookies, the user cannot be authenticated in the system. Therefore, these are essential cookies, without which the system cannot be used. For this reason, they cannot be deactivated. All cookies are limited in time by the browser session. We do not use cookies for tracing, tracking or marketing purposes.

By accepting this privacy policy, you consent to the following cookies being stored on your browser system for a limited period of time.

Cookies in use:

Name	Domain	Procedure	Purpose
x-ms-cpim-admin	main.b2cadmin.ext.azure.com	End of browser session	Contains cross-client user membership data: clients to which a user belongs and the level of membership („admin" or „user").
x-ms-cpim-slice	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	For forwarding requests to the corresponding production instance.
x-ms-cpim-trans	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	To track transactions (number of authentication requests to Azure AD B2C) and the current transaction.
x-ms-cpim-sso:{Id}	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	To manage the session with single sign-on (SSO).
x-ms-cpim-cache:{id}_n	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session, successful authentication	To manage the request status.
x-ms-cpim-csrf	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	Cross-site request token for protection against CSRF attacks.
x-ms-cpim-dc	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	For Azure AD B2C network routing.
x-ms-cpim-ctx	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	Context
x-ms-cpim-rp	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	To save the membership data for the resource provider client.
x-ms-cpim-rc	b2clogin.com, login. microsoftonline.com, company-related domain name	End of browser session	To save the relay cookie.

CMX Portal

We process your personal data in order to provide our Service to you through our platform and for you to be able to access our platform.

The use of our portal is only possible with appropriate registration or for guest users, subject to the CMX terms and conditions, upon invita- tion of an already registered user.

If you register on our platform, we process your personal data in order to process your registration and to be able to provide you with our Services, as well as to comply with the associated rights and obligations. If you place an order, we process your personal data to handle your order and to comply with the associated rights and obligations.

Our platform is reserved exclusively for professionals with sufficient expertise in the relevant field. Therefore, when registering, it may be necessary for you to provide further information in order for us to assess whether you are part of the relevant professional group. The necessary information is marked as mandatory in the registration form. After the positive review of your information, we will process your application and activate your user account.

During the login process, a two-factor authentication is used for the purpose of proof of identity. We use external services for two-factor authentication.

If we have asked for your consent and you have given it, the legal basis for the processing is Art. 6 para. 1 lit. a GDPR. If we have not asked for your consent, the legal basis for the processing is Art. 6 para. 1 lit. f GDPR. Our legitimate interest is the processing and handling of your registration. If the processing is necessary to fulfil a contract with you or to carry out pre contractual measures based on your request, the legal basis for the processing further is Art. 6 para. 1 lit. b GDPR. Recipients of your personal data may be third parties (software and IT service providers, etc.), insofar as this is necessary for the provision of our Service and for the processing of your registration and the associated rights and obligations.

Product change information

We inform registered CMX users about product changes for the purpose of safe use and to inform about changes in possible applications. Such information does not serve for advertising or other marketing purposes. In order to inform you we use the personal data provided during your registration. The legal basis for the processing is Art. 6 para. 1 lit. f GDPR. Our legitimate interest is to provide information on safe use and changes in possibilities. In certain instances, such information may be a legal obligation.

Further links to other websites

Our website may contain links to other websites. Such websites are not covered by this privacy policy and we are not responsible for the privacy practices and/or the content of such other websites. We would like to inform you that the respective privacy policy and further information on data protection of the respective responsible parties apply and must be taken into account.

Depending on the service provider, your data may be transferred and processed outside the European Economic Area (EEA). In addition to the inherent data protection risks associated with such transfer, it may be more difficult to protect and exercise your rights as a data subject.

We have no influence on the further use of your data, which is processed by the respective service provider.

Scope and Amendment of this privacy policy

By using our website and the related offers and services, you consent to the collection and use of your personal data in accordance with this privacy policy. We reserve the right to change this privacy policy and related business practices at any time by uploading updated language on this website. Therefore, please check this page regularly for updates.

Thank you for visiting our website and for taking the time to read this privacy policy.

March, 2023