



AO data privacy notice

Content

-
- 3**
1. Scope
 2. Data protection officer (DPO) at AO
 3. Representative in the EU
 4. Legal basis of data processing
 5. Collection of personal data
-

- 5**
6. Use of personal data
-

- 6**
7. Data transfer and transfer of data abroad
 8. Data retention
-

- 7**
9. Visiting our websites
-

- 19**
10. Your data protection rights
 11. Data security
-

- 20**
12. Amending of this privacy notice
-

1. Scope

AO Foundation is a not-for-profit organization established under the laws of Switzerland with registered domicile at Clavadelerstrasse 8, 7270 Davos, Switzerland. AO Foundation, including all of its affiliated institutions (“AO” or “we” or “our”), are subject to Swiss law and any applicable foreign data protection law and adhere to all other applicable laws and regulations to be considered in its activity.

At AO, we naturally value your privacy highly, and adhere to the applicable privacy laws when collecting and processing your data. Additionally, this data privacy notice is subject to continuous adaptation according to changing regulatory environments and is subject to auditing procedures with regard to accountability. This data privacy notice outlines the principles of data collection and processing for AO. This is not an exhaustive description; other privacy statements (or general terms and conditions, terms and conditions of participation and similar documents) govern specific matters.

This data privacy notice (hereinafter the “privacy notice”) describes how your personal data provided to AO, over the websites of AO Foundation (hereinafter the “AO websites”, see complete list at <https://www.aofoundation.org/websites> list) is handled, namely its collection, storage and usage. Furthermore, it defines how collected personal data may be examined, corrected or deleted.

2. Data protection officer (DPO) at AO

The DPO of AO is a person as named from time to time and is responsible compliance with privacy laws and for resolving your inquiries.

For questions, requests or further information related to data processing by AO, you may send an e-mail to dpo@aofoundation.org. Your questions or requests will be handled by the DPO.

3. Representatives

In the European Union

The representative within the meaning of the GDPR and other national data protection laws of the member states as well as other data protection provisions is:

Swiss Infosec (Deutschland) GmbH

Unter den Linden 24

10117 Berlin

Germany

E-mail: aofoundation.dataprivacy@swissinfosec.de

In the United Kingdom

The representative within the meaning of the UK-GDPR is:

Swiss GRC (UK) Ltd.

The Nova Centre

1 Purser Road

Northampton, Northamptonshire

England

E-mail: aofoundation.dataprivacy@swissgrc.uk.com

4. Legal basis of data processing

As the legal basis for processing your personal data, we always ask for your explicitly stated consent or contractual consent to capture and specifically use your data before collecting or storing it.

Additional purposes can be the performance of a contract which you are a party of, our compliance with legal obligations or obligations set by competent authorities, protection of vital or public interests, or legitimate interests of AO or a third party.

5. Collection of personal data

The following processing principles apply at AO:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Based on information provided by you, the following personal data in particular will be stored:

Identity data

Username, password, user identification (ID), primary e-mail address, professional title, academic title, first name, middle initial, surname, suffix (provides additional information about the person), (second) academic title, gender, date of birth, nationalities.

Contact details

Primary language, organization/hospital, department, unit I (example: maxillofacial unit), unit II (example: division of plastic surgery, foot and ankle surgery), function/job title, courtesy title, address, city, state/province, postal code, country, assistant's name, e-mail address, and phone number, your telephone and fax numbers, mailing/ shipping address, and home address.

Membership data

Home specialty (i.e., AO Spine, AO Trauma, AO CMF, AO VET, AO Recon), membership package, sign-up date, expiration date, award points, status points, associate points, membership status, about me, profile picture, voucher code.

Specialization data

Expertise/specialty, roles, interests.

AO functions/roles

Elected/nominated functions, faculty status (including data for election, nomination processes).

Educational history

Graduation from medical school, board certifications, fellowships, curriculum vitae upload, publication list upload, AO educational event history (event name, type, year, activity levels) and evaluation scores related to AO educational events.

Faculty data

Qualification, institution, academic degree, teaching languages (established year, language proficiency), expertise data (first year surgery involvement, procedures per year, teaching topics), events completed (dates, place, role, evaluation scores, faculty development activities and history).

Travel data

Preferred travel agent, favorite airline(s), favorite airline alliance(s), departure location (airport, city), dietary requests, seating preference, hotel room type, smoking/ nonsmoking preference, car type, passport number, passport issued in (city, country), date passport was issued, passport expiration date, first name in passport, surname in passport, frequent-flyer information, favorite hotel chains, favorite rental companies, additional comments/requirements, accessibility, dietary preference or requests.

Event data

Badge title, organization, first name, surname, pre- and post-event evaluation results, blended learning activities and subsequent results.

Financial data

Reimbursement information: reason for reimbursement (description), city, country, your role, budget provided by, claim, per diem fields, mileage, parking, transport, accommodation (based on respective recent IP system), receipts, bank details (account, bank name, address, account holder name, account number, international bank account number [IBAN], Society for Worldwide Interbank Financial Telecommunications/business identifier code [SWIFT/BIC], other info, comments).

AO stores and uses data deriving from financial transactions on AO websites and shall not be liable for all and any damage caused by disclosing these data to any public authorities upon official request.

Our legal basis for processing the data listed above is your consent and our legitimate interest of pursuing the purposes listed above for data collection, unless we have another legal basis, provided that we require one. Consent given can be withdrawn at any time, but this does not affect data processed prior to withdrawal.

6. Use of personal data

We use store and process personal information based on the legal basis set out in cipher 4 in particular for the following general purposes:

- To enable you to access and use AO services
- To enable you to communicate with other AO website users and/or users of AO services, including but not limited to sending them messages, notifications, or other information
- To operate, protect, improve and optimize AO services and our business, for example by performing analytics, conducting research, personalizing or otherwise customizing user experience, and to provide customer service and support
- To help maintain a trusted environment on AO platforms, such as detection and prevention of actual and potential fraud and other harmful activities, conducting investigations and risk assessments, verifying any identifications provided by you, and conducting checks against databases and information sources for fraud detection and prevention, risk assessment and harm prevention purposes
- To send you service, support and administrative messages, reminders, technical notices, updates, security alerts, and information requested by you
- To send you marketing, advertising, and promotional messages and other information that may be of interest to you, including information about AO, our services, or general promotions for partner

campaigns and services. You can unsubscribe or opt out of receiving these communications in your settings.

- To comply with our legal obligations, resolve any disputes that we may have with any of our users and to enforce our agreements with third parties
- We do not rent or sell your personal data with third parties, except with your consent.

Furthermore, we may use third-party service providers to help us deliver our services and run or analyze AO services (e.g., third-party data analytics services to analyze, among other things, server load). The use by third parties of the data disclosed is strictly limited to the aforementioned purposes.

We also reserve the right to disclose your personal data to (a) comply with relevant laws and regulatory requirements and to respond to lawful requests, court orders, and legal process; (b) to protect and defend our rights or property or those of third parties, including enforcing agreements, policies, and terms of use; (c) in an emergency, including to protect the safety of our employees or any person, or (d) in connection with investigating and preventing fraud.

We also aggregate data into anonymized system usage statistics.

7. Data transfer and transfer of data abroad

We consider the personal data referred to in this privacy notice to be confidential and will treat it accordingly.

We will only pass on your personal data to third parties if:

- You have given your consent
- The disclosure is necessary to assert, exercise or defend legal claims and there is no reason to assume that you have an overriding interest worthy of protection in the nondisclosure of your data
- In the event that a legal obligation exists for the transfer
- The disclosure is within the legitimate interests of us
- This is legally permissible and necessary for the execution of contractual relationships with you

However, we may disclose your personal data to the following categories of recipients for the purposes set out above:

- our service providers (external partner, such as banks, insurances), including processors (such as IT providers);
- dealers, suppliers, subcontractors and other business partners;
- clients;
- domestic and foreign authorities or courts;
- the media;
- the public, including users of our websites and social media;
- industry organizations, associations, organizations and other bodies;
- acquirers or parties interested in the acquisition of business divisions, companies or other parts of AO;
- other parties in possible or pending legal proceedings;
- affiliates of AO.

We reserve the right to transfer, store, use and process your data, including any personal data, to countries outside of Switzerland including the European Economic Area, the United States and possibly other countries. You should note that laws vary from jurisdiction to jurisdiction, so laws and regulations relating to privacy and data disclosure, applicable to the places where your information is

transferred to or stored, used or processed in, may be different from the laws and regulations applicable to your place of residence. We take the legally required safeguards and contractual measures to ensure that any parties we transfer personal data to do so in keeping with the level of data protection and security prescribed by the applicable data protection regulation. If the level of data protection in a country does not correspond to the Swiss or EU standard, we contractually ensure that the protection of your personal data corresponds to that in Switzerland or the EU at all times. To this end, we agree on the EU standard contractual clauses (latest version available [here](#)) with our partners and implement additional technical and organizational measures if necessary.

8. Data retention

We may retain information regarding you and your use of AO services, including personally identifying information and profiling data, for as long as necessary to provide you with our services and the uses described in this privacy notice. Generally, this means that we will keep information for the duration of your account or until the data has fulfilled the purpose for which it was collected.

While AO strives to provide the possibility of a full deletion of personal data, please note that any information that we have copied may remain in backup storage for some period of time after your account deletion.

Notwithstanding the foregoing, we may retain and use such data as necessary to protect our legitimate interests, the interests of third parties or the public, and to comply with our legal obligations, maintain accurate accounting, financial and other operational records, resolve disputes, and enforce our rights connected to your use of AO services.

9. Visiting our websites

In order to display and optimize our website content while ensuring data security, we may collect personal data from you. The same applies to the analysis of website usage and compliance with regulatory and legal requirements. If you use the corresponding functions, we also process personal data to:

- contact you
- regularly inform you about our offers (e.g., newsletter)
- interact with you in connection with our offers and website content (e.g., social media)
- otherwise specified use

Server-Logfiles

When you access one of our websites, the browser used on your end device (e.g., notebook, smartphone, tablet) automatically sends data to the server of the respective website. This data is temporarily stored in a log file, the so-called server log files. The access data includes in particular your IP address, the type of web browser, the operating system used, the date and duration of your visit to our website and the like. This is exclusively information that does not allow any conclusions to be drawn about your person.

The processing of this data is based on our legitimate interests for the purpose of enabling the use of our websites (connection establishment), to ensure system security and stability on a permanent basis, to optimize our offers and for internal statistical purposes. We do not disclose this data to third parties or evaluate it in any other way. A personal user profile is not created.

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of the collection of your personal data for the provision of the website, this is the case when the respective session has ended, but at the latest after 90 days.

Contact

You have the possibility to contact us via e-mail, by mailing, by telephone or by contact form (e.g. when registering for an exam such as the Global Spine Diploma Exam). We usually process your contact data as well as the data you provide us with, in particular content data. If you contact us, the information you provide will be processed for the purpose of handling your request and its processing.

The basis for processing your personal data is our legitimate interest in processing your request. If the contact serves the fulfillment of a contract to which you are a party or the implementation of pre-contractual measures, this is an additional basis for the processing of your personal data.

You can object to this data processing at any time. Please send your objection to the e-mail address mentioned in cipher 2 and we will consider your request. In such a case, your request will not be processed further.

Your personal data will be deleted as soon as your request has been dealt with. This is the case if it can be inferred from the circumstances that the matter in question has been conclusively clarified and the deletion does not conflict with any statutory retention obligations.

Feature Upvote

You also have the ability to provide us with feedback and feature suggestions using an online form. We use Feature Upvote, a service provided by Barbary Software SL, based in Spain ("Barbary"), for this purpose.

The services of Feature Upvote allow us to collect feedback from customers in order to further improve our products. Feature Upvote allows our customers to suggest new features for our products and vote on the suggestions.

In order to send us your feedback or suggestion for improvement, it is necessary that you enter a name and your e-mail address next to your feedback/suggestion. Your email address will not be made public. Barbary will use this information to notify you if your suggestion or comment receives comments, if your suggestion receives upvotes, or if your suggestion is implemented to analyze the suggestion and upvotes.

For more information about the nature, scope and purpose of data processing, please refer to [Feature Upvote's privacy policy](#).

ZenDesk Chat

In order to be able to process user inquiries faster and more efficiently, we use Zendesk Chat, a live chat software of the provider Zendesk Inc. based in the USA, on some of our websites ("Zendesk").

Zendesk allows you to contact us directly (live chat) or send us messages. If you want to use the chat functions, it is necessary to provide a name as well as your e-mail address (live chat). If you would like to send us your message via the chat function, we require further information such as the service concerned or the subject of your inquiry in order to process your request. These mandatory data are required in particular so that we can personally address and contact you and to process your request.

Providing additional data makes it easier for us to process your inquiry and enables us to provide you with more detailed information.

When using the chat, in addition to the information you provide, your IP address and which of our websites you have visited are also recorded. The IP address is anonymized. In addition, Zendesk Chat uses so-called [cookies](#). The information generated by the cookie about your use of our website (including the anonymized IP address) is transmitted to a Zendesk server in the USA and stored there. Conducted chats are logged and stored as well.

For more information on data processing by Zendesk, please see [Zendesk's privacy policy](#).

Working at AO

AO offers an attractive working environment, welcomes innovative ideas, and provides excellent support to help our employees develop further. This includes flexible working arrangements, including home office, a generous package of social benefits, including holiday, pension provision, and global accident insurance. AO is pleased to be able to offer its employees and their families discounts with leading insurance providers.

In order for you to apply for a job at AO, you must open a job application account. For more information on this and on data processing in connection with your application, please refer to the privacy policy that we provide to you upon registration.

WalkMe

On some of our websites we use WalkMe, a service of WalkMe Inc. based in the USA ("WalkMe").

WalkMe provides users of our websites with various assistance and instructions relating to the use of our website respectively its functionalities, for example how to change contact data or newsletter settings. The purpose of WalkMe is to make it easier for you to use our services, and to allow us to track and analyze data about your use of and interactions with our websites on a pseudonymous basis in order to understand how we can improve the design of our websites and improve the help and guidance we provide.

WalkMe uses cookies and similar technologies such as JavaScript and processes data such as your IP address, the location (city/country) from which you use our services, and data about your interactions with our websites.

When using WalkMe, your data may also be processed in countries outside the European Economic Area (EEA), in particular in the USA, which are not considered having an adequate level of data protection. WalkMe declares in its [privacy policy](#) that for data transfers to countries that do not have an adequate level of data protection according to the European Commission, it has taken the necessary measures (e.g. standard contractual clauses) to ensure the protection of your personal data. Although this does not provide a conclusive guarantee of compliance with Swiss data protection law, WalkMe is still certified under the EU-US, respectively Swiss-US [Privacy Shield framework](#).

For more information about WalkMe's privacy and security practices, please see [WalkMe's privacy policy](#) and [website](#).

Raffles

If you take part in raffles, we collect your personal data, which are necessary for carrying out the raffle. This is usually your name and contact details. It may be that we pass on your personal data to

our raffle partners, e.g., in order to send you the prize. Participation in the competition and the associated collection of data is, of course, voluntary. You will find detailed information in our conditions of participation for the respective competition.

By participating in a competition, you agree to receive our newsletter. You can object to this by sending an e-mail to the e-mail address mentioned under cipher 2.

Surveys

In order to improve our services and to better meet the needs of our customers, we occasionally conduct surveys based on your consent. To conduct the surveys, we use SurveyMonkey, a service provided by Momentive Inc. based in the USA or, if you are a resident of the European Economic Area (EEA) or Switzerland, Momentive Europe UC, based in Ireland ("Momotive").

When you take a survey, Momentive collects information about the device and application you use to take the survey. This includes, but is not limited to, your IP address, operating system version, device type, and browser type information. If you use a mobile device to participate, Momentive also collects the device's UUID. Momentive also uses so-called third-party tracking services, which in turn set cookies and web beacons, to collect usage data and user statistics. We have no control over the data collected by Momentive.

We cannot exclude the possibility that the data collected by Momentive may also be transferred to the USA and other countries in which Momentive has offices.

We have entered into a processing agreement with Momentive, including EU standard contractual clauses, to ensure the protection of your personal data and an appropriate level of data protection. In addition, Momentive remains certified under the EU-US and Swiss-US [Privacy Shield agreements](#).

If you have consented to the use of SurveyMonkey, you may revoke your consent at any time with future effect by sending us an email to the email address listed under cipher 2.

For more information, please see SurveyMonkey's [privacy notice](#) and [Terms of Use](#).

Newsletter

We are happy to inform you about the latest news on education and research, calls for grant applications or prestigious positions, events for members and information about your privileges, and much more through our newsletters. If you would like to receive any of the newsletters we offer, we require several pieces of information from you, specifically your first and last name and an e-mail address.

For sending our newsletter and the associated processing of the above-mentioned data, we use the tool Pardot of the service provider Salesforce.com Inc. based in the USA. We have concluded a [data processing agreement](#) with Salesforce in which Salesforce undertakes to comply with the EU standard contractual clauses in the event of data disclosures outside the EU/EEA.

We would like to point out that we also use Pardot to evaluate your user behavior when sending the newsletter. For this purpose, our newsletters and marketing e-mails may contain small, "invisible" files (beacons), via which various evaluations are possible to improve our offers. The data is stored and evaluated in order to better adapt the newsletter dispatch and the advertising mailing to individual interests in the future. We do not pass on this information to third parties. For technical reasons, this information can be assigned to individual newsletter recipients. However, it is neither our intention nor that of the service provider to observe individual users. The evaluations serve us

much more to recognize the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users.

You can revoke your consent to the storage of your data and its use for sending the newsletter at any time, for example via the "unsubscribe" link in the newsletter or by sending an e-mail to the e-mail address mentioned in cipher 2. If you would like to prevent the use of web beacons, please set your mail program so that no HTML is displayed in messages. See the following links for explanations on how to make this setting in the most popular email programs: [Microsoft Outlook](#) and [Mail on Mac](#).

For more information about Salesforce's privacy practices, please visit their "[Privacy Information](#)" webpage.

AO account

With the opening of an AO account, you receive password-protected direct access to your data stored with us. In order for you to be able to register, we require various information from you, such as first and last name, valid e-mail address, field of interest, gender, current country of employment and a password chosen by you. Some data are not mandatory for our rendering of services and can be provided by you on a voluntary basis. Mandatory data is marked accordingly. After providing the required data, you will receive a verification code from us, with which you must confirm your e-mail address.

The data collected is required to provide you with password-protected access to your personal data stored with us and to process your requests. Among other things, you can use your account to manage the receipt of our newsletters, to register for courses, exams and/or events, to manage your orders or your payment methods. In addition, we offer you the possibility to submit a data information request directly through your account.

We will store your data on our servers for as long as necessary to provide the services or information requested by you, unless a longer retention period is necessary based on our legitimate interests or prescribed by law.

Alternatively, you can also register using social networking credentials, such as with your Facebook account, a service by Facebook Inc., based in the USA or Facebook Ireland Ltd., based in Ireland, with your Google account, a service provided Google LLC., based in the USA or Google Ireland Ltd., based in Ireland or Apple account, a service provided by Apple Inc., based in the USA or Apple Distribution International Ltd., based in Ireland. For more information on data processing by the respective social network, please refer to the respective privacy statements:

- [Facebook](#)
- [Google](#)
- [Apple](#)

When logging in with Facebook, Google or Apple, your browser automatically establishes a direct connection with the respective server. To register, you will be redirected to the Facebook, Google or Apple webpage. There you can log in with your user data. This links your user account with Facebook, Google or Apple to our service. We have no influence on the scope and further use of data collected by Facebook, Google or Apple through the use of their login.

We use Facebook, Google and Apple to make the registration and login process easier for you and to shorten it. This is also our legitimate interest in the processing of the above data by the third-party provider. You can prevent the processing of the above information by Facebook, Google or Apple by using our registration mask and not logging in via your Facebook, Google or Apple Account.

Registering a AO account is voluntary and based on your consent. To terminate your AO account, send an e-mail to the e-mail address mentioned in cipher 2.

If you wish to terminate your AO account, the associated data will be deleted, subject to legal retention obligations. It is your responsibility to save your personal data in the event of termination. We are entitled to irretrievably delete all data stored during the term of the contract.

Grants and Fellowships

Our various AO Fellowship Programs (e.g., trauma or craniomaxillofacial) offer a unique educational experience to the most promising young surgeons in their respective specialties. With those programs, we provide a gateway to our worldwide network and networking opportunities across our global community.

Fellows will have the opportunity to learn from leading experts in the carefully selected and renowned centers, covering the entire scope of the respective surgical procedures performed around the world. The duration of a fellowship program is from 6 to 12 weeks.

Before you can apply for a fellowship program, you need an appropriate AO membership (see above, AO account). As the number of possible fellowships is limited, we need the following information from you, among others, in order to select the most suitable candidates. You can upload this information directly to us as part of your application:

- Letter of motivation
- Curriculum vitae
- Copy of your medical school diploma
- Copy of your passport

If we require further information from you as part of the respective application, you can find this in the respective application requirements. If it is necessary to provide personal data of other persons (such as co-investigators), we assume that you have obtained the relevant consents for disclosure to us and ensure that the information provided is correct. This data will only be stored, evaluated, processed or forwarded internally as part of your application. Furthermore, the data may be processed for statistical purposes. In these cases, it is not possible to draw conclusions about individual persons.

Your application data will be processed in order to fulfill our (pre)contractual obligations within the scope of the application process.

You can object to this data processing at any time and withdraw your application. Please send your objection to the e-mail address mentioned in section 2.

If we grant you a fellowship, the transmitted data will be stored for the purpose of processing the fellowship in compliance with the statutory provisions.

If we reject your application, your data will be deleted immediately after rejection.

For more information on our various fellowship programs, please visit the respective websites:

- [AO Trauma](#)
- [AO Spine](#)
- [AO CMF](#)
- [AO Recon](#)
- [AO VET](#)

Cookies / tracking and other techniques regarding the use of AO websites

Cookies

We typically use cookies and similar techniques on our websites, which allow for an identification of your browser or device. A cookie is a small text file that is sent to your computer and automatically saved by the web browser on your computer or mobile device, when you visit our website. If you revisit our website, we may recognize you, even if we do not know your identity. Besides cookies that are only used during a session and deleted after your visit of the website (session cookies), we may use cookies in order to save user configurations and other information for a certain time period (permanent cookies).

Apart from technically mandatory cookies, we only use cookies if you have given us your consent to do so. You can revoke any consent given at any time by changing your [cookie settings](#).

Notwithstanding the foregoing, you may configure your browser settings in a way that it rejects cookies, only saves them for one session or deletes them prematurely. Most browsers are preset to accept cookies. We use permanent cookies in order to understand how you use our services and content. If you block cookies, it is possible that certain functions are no longer available to you. By accepting the cookies and using our websites, you consent to the use of such techniques. If you object, you must configure your browser or e-mail program accordingly and/or revoke your consent.

Google Services

On our websites, we use various services of Google LLC, based in the USA, respectively if you have your habitual residence in the European Economic Area (EEA) or Switzerland, Google Ireland Limited, based in Ireland ("Google"). The processing of personal data when using "Google Maps" always takes place in the USA. We use the following Google services on our websites:

- Google Tag Manager
- Google Analytics
- Google Ads
- Google Optimize
- Google Marketing Platform
- Google reCAPTCHA

You can find more information about the individual services below.

Google uses technologies such as cookies, web storage in the browser and tracking pixels, which enable an analysis of your use of our websites. The information thus generated about your use of our website may be transmitted to a Google server in the USA and stored there.

We use tools provided by Google that Google claims can process personal data in countries where Google or [Google's subcontractors](#) maintain facilities. Google promises an adequate level of data protection in its [Data Processing Addendum for Products where Google is a Data Processor](#) by relying on the EU standard contractual clauses. Although this does not provide a conclusive guarantee of compliance with Swiss or European data protection law, Google is also certified under the [Swiss-U.S. and EU-.US. Privacy Shield framework](#).

For more information about Google's processing and privacy settings, please refer to [Google's privacy policy](#) respectively [privacy settings](#).

Google Tag Manager

Our websites use the Google Tag Manager. With the Google Tag Manager, website tags can be managed efficiently. Website tags are placeholders that are stored in the source code of the respective website, e.g. to record the integration of frequently used website elements, such as code for web analytics services. Google Tag Manager does not use cookies and triggers other tags, which in turn may collect data. Google Tag Manager does not access this data. If a deactivation has been made at the domain or cookie level, this remains in place for all tracking tags that are implemented with Google Tag Manager. For more information, see the [Google Tag Manager Terms of Service](#) and [Google's Tag Manger Help Center](#).

Google Analytics

For the purpose of analyzing our websites and their visitors as well as for marketing and advertising purposes, we use the web analytics service Google Analytics. Google Analytics uses cookies that are stored on your end device (laptop, tablet, smartphone or similar) and enable an analysis of your use of our website. This enables us to evaluate the usage behavior on our website and to make our offer more interesting by means of the statistics/reports obtained.

The information generated by the cookie about your use of our website (including your IP address) is usually transmitted to a Google server in the U.S. or Ireland and stored there.

Google Analytics 4 has IP address anonymization enabled by default. This means that your IP address is shortened by Google within Switzerland or the EU/EEA before being transmitted to the USA. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there.

Google uses this information to evaluate your pseudonymous use of our website, to compile reports on website activity and to provide us with other services related to website and internet use. The IP address transmitted by your browser as part of Google Analytics will not be merged with other Google data, according to Google. When you visit our website, your user behavior is recorded in the form of events (such as page views, language settings, your "click path", interaction with the website) as well as other data such as your approximate location (region), technical information about your browser and the end devices you use or the referrer URL, i.e. via which website / advertising material you came to our website.

As an alternative to objecting to any consent given (by changing your [cookie settings](#)), you can prevent the collection of data generated by the cookie and related to your website use (including your IP address) to Google and the processing of this data by Google by downloading and installing the [Google Analytics Opt-out Browser Add-on](#).

This will set an opt-out cookie that will prevent future collection of your data when you visit our website. To prevent the collection of data by Google Analytics across different devices, you must perform the opt-out on all devices used.

An overview of the data use in Google Analytics and the measures taken by Google to protect your data can be found in [Google's Help Center](#).

Further information on the terms of use of Google Analytics and data protection at Google can be found in the [Google Analytics Terms of Service](#) and [Google's privacy policy](#).

Google Ads

With Google Ads, a cookie is set on your computer ("conversion cookie") if you have reached our websites via a Google ad. These cookies have a limited validity, do not contain any personal data according to Google and are therefore not used for personal identification. If you visit certain of our websites and the cookie has not yet expired, we and Google can recognize that you clicked on the ad and were thus redirected to our websites. Each Google Ads customer receives a different cookie. Thus, there is no way that cookies can be tracked across Ads customers' websites. The information collected with the help of the conversion cookie is used by Google to create conversion statistics for Ads customers who have opted for conversion tracking. These statistics tell us the total number of users who clicked on our ads and which of our websites were subsequently visited by the respective user. We do not receive any information with which you can be personally identified.

On the basis of the information collected, your browser is assigned categories that are relevant to your interests. These categories are used for the placement of interest-related advertising.

We use the data acquired about you with the above-mentioned cookie (so-called conversion tracking) for the following purposes:

- Remarketing
- target groups with common interests
- user-defined target groups with common interests
- target groups ready to buy
- similar target groups
- demographic and geographic targeting
- user lists

By using Google Ads, we reach users who have already visited our websites. This allows us to present our advertising to target groups who are already interested in our products or services.

For more information about Google's advertising technology and the use of cookies by Google, please visit [Google's website](#).

Google Optimize

We also use the Google marketing service "Google Optimizer". Google Optimizer allows us to track the effects of various changes to a website (e.g. changes to the input fields, the design, etc.) as part of so-called "A/B testing". For these testing purposes, cookies are stored on your devices. Only pseudonymous data about you will be processed. For more information about Google Optimizer, please visit: <https://optimize.google.com/optimize/home/>.

Google Marketing Platform

The online marketing tool Google Marketing Platform ("GMP") uses cookies to serve ads that are relevant to users, to improve campaign performance reports, or to prevent a user from seeing the same ads more than once. Using a Cookie ID, Google records which ads are served in which browser and can thus prevent them from being displayed more than once.

In addition, GMP can use cookie IDs to record so-called conversions, i.e. whether a user sees a GMP ad and later calls up the advertiser's website and makes a purchase there. According to Google, GMP cookies do not contain any personal information.

Your browser automatically establishes a direct connection with Google's server. We have no influence on the scope and further use of the data collected by Google through the use of this service. According to Google, by integrating GMP, Google receives the information that you have called up the relevant part of our websites or clicked on an advertisement from us. If you are registered with a Google service, Google can assign the visit to your user account. Even if you are not registered with Google or have not logged in, there is a possibility that the provider may obtain and store your IP address. The use of GMP may also result in the transmission of personal data to Google's servers in the USA.

You can find more information about GMP on the [Google Marketing Platform website](#).

Google reCAPTCHA

The reCAPTCHA function is used to distinguish whether an entry (e.g. in a contact form) is made by a human or automatically by a computer program (so-called [bots](#)). In this way, we want to ensure the security of our websites and protect them in particular from automated entries (or attacks) and from spam. The processing is thus based on our legitimate interests.

For this purpose, reCAPTCHA analyzes the behavior of the website visitor on the basis of various characteristics. These analyses run completely in the background and begin automatically as soon as you visit our websites. To differentiate between humans and bots, Google analyzes various information, such as the IP address of the end device used, time spent on the website, the browser and operating system used or mouse movements made by the website visitor.

For more information on the use of the data collected by Google, please refer to [the privacy policy](#) and [Google's terms of service](#).

LinkedIn Marketing Solutions

On our websites, we use LinkedIn Marketing Solutions ("LMS"), a service of the LinkedIn Corporation based in the USA, or if you have your habitual residence in the European Economic Area (EEA) or Switzerland, LinkedIn Ireland Unlimited Company based in Ireland ("LinkedIn").

LMS stores and processes information about your user behavior on our websites. For this purpose, LMS uses, among other things, cookies that are stored locally in the cache of your web browser on the respective end device used by you and enable an analysis of your use of our websites.

We use LMS for marketing and optimization purposes, in particular to analyze the use of our websites, to continuously improve individual functions and offers as well as the user experience and to place relevant and interesting ads for you. In particular, we use the LinkedIn Insight tag, which allows us to track conversions, retarget our website visitors, and gain additional information about the LinkedIn members who view our ads.

If you are logged into the member area of LinkedIn, LinkedIn can assign the use of our online offer to your profile. If you do not wish this, you must log out of LinkedIn before visiting our websites.

Further information on the type, purpose and scope of data processing can be found in [LinkedIn's privacy policy](#), the [cookie policy](#) and [privacy management portal](#). Furthermore, you can object to personalized (LinkedIn) advertising by installing an [opt-out cookie](#), regardless of whether you are a LinkedIn member or not.

Meta-Pixel, Custom Audiences and Conversions

Our websites uses Meta Pixel, a service provided by Meta Platforms Inc. based in the USA respectively if you have your habitual residence in the European Economic Area (EEA) or Switzerland Meta Platforms Ireland Ltd. based in Ireland ("Meta"). Instagram and Facebook are services provided by Meta.

With the help of the Meta Pixel, it is possible for Meta to determine the visitors to our websites as the target group for the display of ads (so-called "Facebook Ads" or "Instagram Ads"). Accordingly, we use the meta pixel to display the Facebook and Instagram ads placed by us only to those Facebook and/or Instagram users who have shown an interest in our online offers or have certain characteristics (e.g. interests in certain topics or products determined on the basis of the websites visited), which we transmit to Meta (so-called "Custom Audiences"). With the help of the Meta Pixel, we want to ensure that our Facebook and Instagram Ads correspond to the potential interest of users and do not have a harassing effect.

Furthermore, the Meta Pixel allows us to track the effectiveness of our Facebook- and Instagram Ads for statistical and market research purposes by seeing whether users are redirected to our website after clicking on a Facebook- or Instagram Ad (so-called "conversions").

Furthermore, we use the additional function "automatic advanced matching" when using the Meta Pixel. Here, data such as telephone numbers, e-mail addresses, dates of birth or postal codes are sent to Meta in encrypted form as additional information, provided that you have made this data available to us. This enables us to increase the number of assigned "conversions" and to enlarge our "Custom Audiences". You can find further information on "automatic extended matching" in Meta's corresponding [help section](#).

We also use the "Custom Audiences from customer lists" method. This allows us to upload various customer information, such as E-mail addresses, telephone numbers, first and last names, to Meta in encrypted form. With the help of this information, Meta can determine whether someone should be added to our advertising target group on Facebook or Instagram. We do this to ensure that ads are only shown to users who have an interest in our information and services. Further information on Custom Audiences from customer lists can be found in the relevant [help section](#) of Meta.

Through the use of cookies, Meta can subsequently recognize you in the member area of Facebook or Instagram and optimize the efficiency of advertisements, e.g. by offering advertisements targeted to specific groups. The prerequisite for this is that you are logged into the member area of Facebook or Instagram. If you are not a member of Facebook or Instagram, you are not affected by this data processing.

General information about the use of data by Meta, about your rights in this regard and options for protecting your privacy can be found in Meta's data policy, available on the website of [Facebook](#), respectively [Instagram](#). Specific information and details about the Meta pixel and how it works can be found in Meta's [help section](#). If you generally want to object to the collection by Meta Pixel and the use of your data for the display of Facebook or Instagram ads, you can do so using [Facebook's Ad Settings](#) or [Instagram's privacy settings](#). To do this, you must be logged in on Facebook respectively Instagram.

Social media plugins

We use social media plugins from various social networks on our websites. These social media plugins may be, for example, the «Like button» or other functionalities, e.g., sharing content of the

websites on social networks. You can recognize the social media plugins by the logos of the social networks concerned.

When you activate the respective plugin by clicking on the associated button (consent) a direct connection to the provider's server is established. As soon as you activate the plugin, the respective provider receives the information that you have visited our websites with your IP address. If you are logged in to your respective social media account (e.g., Facebook) at the same time, the respective provider can assign the visit of our websites to your user account. If you want to prevent this, you should log out before clicking on the plugin. An assignment is made in any case when you log in to the respective network after clicking on the plugin.

If you have your habitual residence in Switzerland or the EEA, the provider of the plugins is based in Ireland, otherwise in the USA. The processing of personal data when using Vimeo's plugins always takes place in the USA. We have integrated plugins from the following social networks into our websites:

- [Facebook](#)
Meta Platforms Inc. (USA)/Meta Platforms Ireland Ltd. (Ireland): [Privacy Policy](#)
- [Instagram](#)
Meta Platforms Inc. (USA)/Meta Platforms Ireland Ltd. (Ireland): [Privacy Policy](#)
- [LinkedIn](#)
LinkedIn Corporation (USA)/LinkedIn Ireland Unlimited Company (Ireland): [Privacy Policy](#)
- [Twitter](#)
Twitter Inc. (USA)/Twitter International Company (Ireland): [Privacy Policy](#)
- [Vimeo](#)
Vimeo Inc. (USA): [Privacy Policy](#)
<https://vimeo.com/privacy>

Social media presence

On our websites, we have set up links to our social media presence on Facebook, Instagram, LinkedIn, Twitter, YouTube, Vimeo and SoundCloud.

If you click on the corresponding icons of the social networks, you will automatically be redirected to our profile on the respective social network. In order to be able to use the functions of the respective network there, you must partially log in to your user account for the respective network.

When you open a link to one of our social media profiles, a direct connection is established between your browser and the server of the social network in question. This provides the network with the information that you have visited our websites with your IP address and accessed the link. If you access a link to a network while logged in to your account on the network concerned, the content of our site may be linked to your profile on the network, i.e., the network may link your visit to our websites directly to your user account. If you want to prevent this, you should log out before clicking on the relevant links. In any case, an association takes place when you log in to the relevant network after clicking on the link.

If you have your habitual residence in Switzerland or the EEA, the provider of the social network is based in Ireland, otherwise in the USA. The processing of personal data when using "Vimeo" or "YouTube" always takes place in the USA. More detailed information on data processing by the provider of the social media platform can be found in the privacy policy of the respective provider:

- [Facebook](#)
Meta Platforms Inc. (USA)/Meta Platforms Ireland Ltd. (Ireland): [Privacy Policy](#)
- [Instagram](#)

- Meta Platforms Inc. (USA)/Meta Platforms Ireland Ltd. (Ireland): [Privacy Policy](#)
- [LinkedIn](#)
LinkedIn Corporation (USA)/LinkedIn Ireland Unlimited Company (Ireland): [Privacy Policy](#)
- [Twitter](#)
Twitter Inc. (USA)/Twitter International Company (Ireland): [Privacy Policy](#)
- [YouTube](#)
YouTube LLC (USA): [Privacy Policy](#)
- [Vimeo](#)
Vimeo Inc. (USA): [Privacy Policy](#)
<https://vimeo.com/privacy>

Integration of videos

To integrate videos on our websites, we use the services of the following providers:

- YouTube LLC based in the USA, a subsidiary of Google LLC
- Vimeo Inc. based in the USA
- Kaltura Inc. based in the USA

You can find more information about the individual services below.

YouTube

When you start a YouTube video on one of our websites, a connection to the YouTube servers is established. This lets the YouTube server know which of our pages you have visited. This information (including your IP address) may be transmitted to a Google server in the USA and stored there. If you are logged into your YouTube account at the same time, you enable YouTube to assign your surfing behavior directly to your personal profile. You can prevent this by logging out of your YouTube account before visiting our website.

For more information, please refer to [YouTube's terms of service](#) and the [privacy policy of Google](#).

Vimeo

When you visit one of our websites on which a Vimeo video is embedded, a connection to the Vimeo servers is established. This lets Vimeo's servers know which of our websites you've visited. If you are logged in as a member of Vimeo, Vimeo assigns this information to your personal user account. When you click on the start button of a video, this information can also be assigned to an existing user account. You can prevent this assignment by logging out of your Vimeo user account before using our website and deleting the corresponding cookies from Vimeo.

For more information on data processing and privacy notices, please refer to [Vimeo's privacy policy](#).

We would like to point out that Vimeo may use Google Analytics and refer you to [Google's privacy policy](#) as well as [the opt-out option for Google Analytics](#) or [Google's ad personalization settings](#).

Kaltura

We also use a video player on our websites to play videos that are not stored on our servers. When you visit a website with an embedded Kaltura video, a connection to Kaltura's servers is automatically established. In the process, content is loaded and the corresponding videos are made available. This provides Kaltura with the information which of our websites you have accessed, as well as the usage data that is technically necessary in this context. Kaltura may store this information as well as anonymized information about the activities and frequency of use on its servers in the USA. In addition, cookies are used, for example, to save settings that have been made.

In accordance with the privacy policy, Kaltura does not disclose your data to third parties as a matter of principle, with the exception of those partners who provide part of the services and functions of the Kaltura platform. Your data may also be disclosed to third parties if, for example, Kaltura is required to do so by law or to assert/defend claims.

If Kaltura discloses your Personal Data in a country that is insecure from a data protection perspective (such as the USA), it will ensure, in accordance with its [privacy policy](#), that the recipient of your Personal Data takes appropriate security precautions, including by entering into data processing contracts that include, where applicable, standard contractual clauses or an alternative mechanism for the transfer of Personal Data that has been approved by the European Commission or other applicable supervisory authority.

We have no influence on the further data processing by Kaltura. For more information on data protection and data processing by Kaltura, please refer to their [privacy policy](#).

Links to third-party websites

Our websites may contain links to other websites which are not operated by us and to which this privacy notice does not apply. After clicking on the link, we no longer have any influence on the processing of any data transmitted to third parties (such as the IP address or the URL), as the behavior of third parties is naturally beyond our control. Therefore, we cannot assume any liability for these third-party contents. The respective provider or operator of the pages is always responsible for the content of the linked pages. In this regard, please note the privacy policies of the respective website operators.

10. Your data protection rights

You are generally entitled to the rights of access, rectification, erasure, restriction, data portability, objection to processing and revocation of consent with regard to your personal data.

If you believe that the processing of your personal data violates data protection law or that your data protection rights have been violated in any other way, you can also complain to the supervisory authority. In Switzerland, this is the Federal Data Protection and Information Commissioner (FDPIC).

For this purpose and for questions, suggestions and requests, please contact dpo@aofoundation.org.

Please note that exceptions apply to these rights. In particular, we may be obliged to further process and store your personal data in order to fulfill a contract with you, to protect our own legitimate interests, such as the assertion, exercise or defense of legal claims, or to comply with legal obligations. Also, legitimate interests of third parties or legitimate public interests may lead to a further processing of your personal data. In these cases, we can or must reject certain requests or comply with them only to a limited extent.

11. Data security

We use several tools (encryption, passwords, physical security, etc.) in order to protect your personal data against unauthorized access and disclosure.

We take reasonable technical and organizational precautions to prevent the loss, misuse or alteration of your personal data. Accordingly, we store all the personal data that you provide on secure (password- and firewall-protected) servers.

You also acknowledge that no technical and organizational measures can fully eliminate security risks connected with the transmission of information over the internet. We therefore cannot guarantee the security of data sent over the internet. We use the common secure socket layer (SSL) method in connection with the highest level of encryption supported by your browser. Usually this is a 256-bit encryption. If your browser does not support 256-bit encryption, we use 128-bit v3 technology instead. Whether a single page of AO websites is transmitted in encrypted form is indicated by the closed display of the key or lock symbol in the lower status bar of your browser.

We also use suitable technical and organizational security measures to protect your data against accidental or intentional manipulation, partial or complete loss, destruction, or unauthorized access by third parties. Our security measures are continuously improved in line with technological developments. You are responsible for keeping the account information (username/password) for accessing AO services confidential.

12. Amending of this privacy notice

AO reserves the right to modify this privacy notice at any time, without giving reasons. The current version published on our website shall apply. If the privacy notice is part of an agreement with you, we will notify you by e-mail or other appropriate means in case of an amendment and your consent will need to be renewed upon major changes and in general regularly from time to time.

Version 2.0



AO Foundation
Clavadelerstrasse 8
7270 Davos Platz
Switzerland
Phone +41 81 414 21 11
foundation@aofoundation.org
aofoundation.org