

Data protection for users of the website

Personal Data

When visiting our website, you will not be asked to provide any personal information at any time, neither before accessing nor while using our pages.

Statistical Data

For technical reasons, the following information is stored in a log file when accessing this website:

- Domain from which the access occurred (usually the domain of your internet provider)
- Date and time of access
- Name of the accessed file
- Name and version of the browser used
- Amount of data transferred
- Message indicating whether the access was successful

Our server only registers the domain from which the access occurs during each visit; individual user identifiers (e.g., email address or IP address) are not recorded. A personal reference is not possible.

These statistical data are deleted after 6 weeks. The log data is neither analyzed nor otherwise used or processed. No data is shared with third parties.

This data is also generated when accessing any other website on the internet. Therefore, it is not a specific function of the website offered by imos AG. Such information is collected exclusively in an anonymized form.

Cookies and Used Technologies

Our website automatically collects session cookies to ensure the error-free provision of the web pages. For technical reasons, it is not possible for us to disable these cookies (see also "Personal Data").

Consent Tool Klaro

We use the open-source cookie consent technology "Klaro" on our website, provided by KIProtect GmbH, Bismarckstr. 10-12, 10625 Berlin.

Klaro stores your given consents for the use of cookies and, according to its own statements, does not use them itself.

You can change the consent data yourself at any time.

Further information on data processing by Klaro can be found at: <https://heyklaro.com/de/ressourcen/datenschutz>

The legal basis for using the open-source cookie consent technology Klaro is Art. 6 para. 1 lit. c GDPR.

Google Analytics

We use features of the web analytics service Google Analytics, operated by Google Inc., 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. Google Analytics uses so-called "cookies," which are text files stored on your computer that enable an analysis of your use of the website. The information generated by the cookie about your use of this website is usually transmitted to a Google server in the USA and stored there. Google is responsible for the data's privacy-compliant handling and is certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. We have no influence on the data stored. Google is responsible for the privacy-compliant handling of the data. If IP anonymization is activated on this website, your IP address will be truncated by Google within member states of the European Union or other parties to the Agreement on the European Economic Area. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and truncated there. On our behalf, Google will use this information to evaluate your use of the website, compile reports on website activity, and provide other services related to website and internet usage to the website operator. The IP address transmitted by your browser as part of Google Analytics will not be merged with other Google data. You can prevent the storage of cookies by adjusting your browser software settings accordingly; however, we point out that in this case, you may not be able to use all the functions of this website to their full extent. You can also prevent the collection of data related to your use of the website (including your IP address) by Google and the processing of this data by Google by downloading and installing the browser plugin available at the following link (<http://tools.google.com/dlpage/gaoptout?hl=de>).

Google Analytics is used for the statistical recording of website usage to continuously improve our website and offerings.

YouTube

On our website, we use the embedding of videos via YouTube and their plugins. YouTube is a service of YouTube LLC, 901 Cherry Ave., San Bruno, CA 94066, USA. YouTube LLC is a subsidiary of Google LLC, 1600 Amphitheatre Pkwy, Mountain View, CA 94043, United States. We use the services of YouTube LLC, which run through the Google server of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

The embedding of videos and plugins from YouTube is done via iFrame. Only by activating (so-called two-click solution) the video plugin do you establish a connection to the YouTube or Google servers and activate the content. When loading the services, YouTube or Google may collect and process information (including personal data). We cannot exclude that YouTube or Google also transmits the information to a server in a third country. Google is responsible for the privacy-compliant handling of the data and is certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. Further information on YouTube or Google's privacy policies can be found at www.google.com/policies/privacy/.

Due to the embedding of YouTube, you can instantly view the videos we provide directly on our website.

The provision of personal data is neither legally nor contractually required nor necessary for a contract conclusion. You are also not obliged to provide personal data. However, the non-provision may result in you not being able to use our website or not being able to use it to its full extent.

Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

We want to inform you once again that, in addition to the data described above collected by YouTube or Google, all data stored by you in your Google account will also be collected when you access our website with a logged-in Google account. We have no influence on the data collected at this point.

Furthermore, you can also log out of your account to prevent further data collection by Google.

Use of Vimeo

On our website, we use Vimeo and the analytics tool involved in it. Vimeo is a video platform operated by Vimeo.com, Inc., 555 West 18th Street, 10011 New York, United States of America.

We use Vimeo to provide you with our videos on various topics (e.g., training). The analysis is used to continuously improve our videos.

The provision of personal data is neither legally nor contractually required nor necessary for a contract conclusion. You are also not obliged to provide personal data. However, the non-provision may result in you not being able to use our website or not being able to use it to its full extent.

The following information is collected and stored:

- IP address
- Cookie ID
- Referrer URL
- Current URL
- Browser type
- Device information
- Web activity
- Session duration
- Bounce rate
- Other information you have provided in your Vimeo account if you are logged in

The legal basis for processing personal data is Art. 6 para. 1 lit. a GDPR. The collected data will be deleted as soon as they are no longer required for processing purposes.

We have entered into Standard Contractual Clauses with Vimeo to protect your data as best as possible. Vimeo is also certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. We have no influence on the data stored. Vimeo is responsible for the privacy-compliant handling of the data. However, for analysis purposes, Vimeo may share your data with third parties who also have corresponding contracts with Vimeo.

You have the right to revoke your consent at any time without justification here: <https://www.imos3d.com/datenschutzbestimmungen/>

Further information on Vimeo's privacy policies can be found at <https://vimeo.com/privacy>

Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

We want to inform you once again that, in addition to the data described above collected by Vimeo, all data stored by you in your Vimeo account will also be collected when you access our website with a logged-in Vimeo account. We have no influence on the data collected at this point.

Furthermore, you can also log out of your account to prevent further data collection by Vimeo.

Use of LinkedIn

On our website, we have linked our LinkedIn page. LinkedIn is a web-based social network operated by LinkedIn, 1000 W Maude, Sunnyvale, CA 94085, United States of America. We are registered for the branch office LinkedIn Germany, Sendlinger Straße 12, 80331 Munich, Germany.

We use LinkedIn for advertising, information, and recruiting. Personal data is collected by LinkedIn as soon as you access our LinkedIn page. We have no influence on the scope of data collected by LinkedIn.

We cannot exclude that personal data may be transmitted to LinkedIn when accessing the website. At the latest, personal data will be collected by LinkedIn when accessing our LinkedIn page. We also cannot exclude that LinkedIn transmits the information to a server in a third country.

The provision of personal data is neither legally nor contractually required nor necessary for a contract conclusion. You are also not obliged to provide personal data. However, the non-provision may result in you not being able to use our website or not being able to use it to its full extent.

We have entered into Standard Contractual Clauses with LinkedIn to protect your data as best as possible. LinkedIn is also certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering

to these data protection standards. We have no influence on the data stored. For analysis purposes, LinkedIn may share your data with third parties who also have corresponding contracts with LinkedIn.

Further information on LinkedIn's privacy policies can be found at https://de.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy.

Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

We want to inform you once again that, in addition to the data described above collected by LinkedIn, all data stored by you in your LinkedIn account will also be collected when you access our website with a logged-in LinkedIn account. We have no influence on the data collected at this point.

Furthermore, you can also log out of your account to prevent further data collection by LinkedIn.

Use of Facebook

On our website, we have linked Facebook. Facebook is a social network of Meta Platforms Inc. (formerly Facebook Inc.), 1 Hacker Way, Menlo Park, CA 94025, United States of America. We host Facebook from the branch office Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

We use Facebook for public relations, information, communication, and advertising. Personal data is collected by Facebook as soon as you access our Facebook page. We have no influence on the scope of data collected by Facebook.

We cannot exclude that personal data may be transmitted to Facebook when accessing the website. At the latest, personal data will be collected by Facebook when accessing our Facebook page. We also cannot exclude that Facebook transmits the information to a server in a third country.

The responsibility for personal data collected on the Facebook page lies entirely with Facebook.

Further information on Facebook's privacy policies can be found at <https://www.facebook.com/policy.php/>.

We have entered into Standard Contractual Clauses with Meta to protect your data as best as possible. Facebook is also certified under the EU-US Data Privacy Framework

(DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. We have no influence on the data stored. For analysis purposes, Meta may share your data with third parties who also have corresponding contracts with Meta.

Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

We want to inform you once again that, in addition to the data described above collected by Meta services, all data stored by you in your Facebook account will also be collected when you access our website with a logged-in Facebook account. We have no influence on the data collected at this point.

Furthermore, you can also log out of your account to prevent further data collection by Facebook.

Use of Instagram

On our website, we have linked Instagram. Instagram is a social network of Meta Platforms Inc. (formerly Facebook Inc.), 1 Hacker Way, Menlo Park, CA 94025, United States of America.

We use Instagram for public relations, advertising, information, and communication, sharing photos and videos, commenting and favoriting posts, sending messages, and subscribing to profiles and pages. Personal data is collected by Instagram as soon as you access our Instagram page. We have no influence on the scope of data collected by Instagram.

We cannot exclude that personal data may be transmitted to Instagram when accessing the website. At the latest, personal data will be collected by Instagram when accessing our Instagram page. We also cannot exclude that Instagram transmits the information to a server in a third country.

The responsibility for personal data collected on the Instagram page lies entirely with Instagram.

Further information on Instagram's privacy policies can be found at <https://www.privacycenter.instagram.com/policy/>.

We have entered into Standard Contractual Clauses with Meta to protect your data as best as possible. Meta is also certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. We have no influence on the data stored. For analysis purposes, Meta may share your data with third parties who also have corresponding contracts with Meta.

Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

We want to inform you once again that, in addition to the data described above collected by Meta services, all data stored by you in your Instagram account will also be collected when you access our website with a logged-in Instagram account. We have no influence on the data collected at this point.

Furthermore, you can also log out of your account to prevent further data collection by Instagram.

Use of Cloudflare

On our website, we use the Content Delivery Network ("CDN") service Cloudflare. Cloudflare is a globally distributed CDN including DNS services provided by Cloudflare Inc., 10 Townsend St., San Francisco, CA 94107, United States of America. The use of Cloudflare enables us to provide you with our website very quickly. This is made possible by Cloudflare because our website is mirrored on all Cloudflare servers and accessed from the server with the least traffic at the time. Due to communication with other servers, we cannot guarantee that personal data will not be stored and processed in third countries. Cloudflare Inc. explains that your data is only processed in the United States of America and the European Economic Area (EU, Switzerland, United Kingdom), but we have no influence on this. Further information on data processing by Cloudflare Inc. can be found at <https://www.cloudflare.com/privacypolicy/>.

The following information is collected and stored through the use of Cloudflare:

- IP address
- Device information
- Browser information
- Cookie ID

- Referrer URL
- Status information
- Timestamp
- Operating system
- Transferred data volume
- Log data

The legal basis for processing personal data is Art. 6 para. 1 lit. f GDPR. The collected data will be deleted as soon as they are no longer required for processing purposes. We have entered into Standard Contractual Clauses with Cloudflare to protect your data as best as possible. Cloudflare is also certified under the EU-US Data Privacy Framework (DPF). The EU-US Data Privacy Framework (DPF) is an agreement between the European Union (EU) and the USA that aims to ensure compliance with European data protection standards in the USA. Each company certified under this standard commits to adhering to these data protection standards. We have no influence on the data stored. For analysis purposes, Cloudflare may share your data with third parties who also have corresponding contracts with Cloudflare. If you do not want to use Cloudflare, you must disable the execution of script codes in your browser or integrate a script blocker for your browser. However, this may result in you not being able to use our website or not being able to use it to its full extent. This may also apply to other websites. Please note that this service may transfer the collected data to another country. This country may also be outside the European Union and the European Economic Area and therefore may not provide an adequate level of data protection. If the data is transferred to the United States of America, there is a risk that your data may be viewed and processed by US authorities for monitoring and surveillance purposes. In this case, you have no legal remedies to protect your data.

Use of CAPTCHA

On our website, we use CAPTCHAs to protect it from spam, automated attacks, and abusive access. Technically, these are CAPTCHAs ("Completely Automated Public Turing Test to Tell Computers and Humans Apart") designed to distinguish between human users and automated programs. We do not use any external service for the CAPTCHAs. The CAPTCHAs are loaded directly from our server.

Social Media Services

The integration of social media services is done solely through linking.

When visiting our pages on social media services, where we inform about our activities and services, present ourselves, and want to communicate with all interested parties, certain information about you is processed.

Unfortunately, we cannot influence the processing of personal data, as social media services determine this.

As the operator of the page, we have no interest in collecting and further processing your individual personal data for analysis or marketing purposes by the social media operator.

SSL/TSL Encryption

We use SSL/TSL encryption for security reasons and to protect the transmission of confidential content. You can recognize an encrypted connection by the browser's address line. If it is an SSL/TSL-encrypted page, the address line begins with "https."

Hosting

We host our website on our own server in Germany.

Use of Personal Data

When you contact us, you agree that your data will be stored and used by us. All data is processed in compliance with the General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG-new), and other legal provisions. Your legitimate interests are considered in accordance with legal requirements. Your data will always be treated confidentially.

If you send us an email, it and your email address will only be used for correspondence with you.

Personal data transmitted to us, such as name, address, telephone number, bank details, or email address, will only be collected, processed, and used for the following purposes and only to the extent necessary for each purpose:

- To process your inquiries
- For the purpose of contract execution
- For prospect management, customer acquisition, and customer care
- To provide services
- For marketing purposes

Right to Data Portability

Data that we collect based on your consent or process automatically in fulfillment of a contract can be handed over to you or a third party in a common, machine-readable

format. If you exercise this right and request the direct transfer of the data to another responsible party, this will only be done if it is technically feasible.

Deletion Periods

All personal data is only stored by us as long as it is required for the respective purpose, we are legally obligated to store it, or it is permissible under a legal regulation.

Right to Information, Correction, Blocking, and Deletion

Upon request, we will inform you as soon as possible in writing, in accordance with applicable law, whether and which personal data about you is stored with us.

If incorrect information is stored despite our efforts to ensure data accuracy and timeliness, we will correct it at your request. If you wish for blocking or deletion, please contact us.

Consent / Revocation of Consent

If you have given consent to store and process your data, you can revoke your consent at any time with effect for the future. A simple email to info@imos3d.com is sufficient. The legality of the data processing carried out until the revocation remains unaffected by the revocation.

Security

The **imos AG** uses technical and organizational security measures to protect your personal data provided to us from accidental or intentional manipulation, loss, destruction, and unauthorized access by third parties.

Our security measures are continuously improved and adapted in line with technological developments.

Contact for Data Protection Questions and Complaints

For questions, information, requests, or complaints regarding data protection, please contact our data protection officer:

Matthias Jasinski, jasinski**NET**

Alter Markt 16

32052 Herford

Tel.: 05221.282 0070

datenschutz@jasinskinet.de

You have the right at any time to free information, correction, blocking, and, if necessary, deletion of your stored data. Please contact info@imos3d.com or send us your request by post or fax.

Name and Address of the Responsible Party:

imos AG

Planckstraße 24

32052 Herford

Phone: 05221.976-0

Fax: 05221.976-123

The responsible party is the natural or legal person who alone or jointly with others determines the purposes and means of processing personal data (e.g., name, address, email address).

You have the right to lodge a complaint with the competent supervisory authority in case of data protection violations. The supervisory authority for data protection questions and complaints regarding us is:

State Commissioner for Data Protection and Freedom of Information

North Rhine-Westphalia

Postfach 20 04 44

40102 Düsseldorf

Tel.: 0211.38424-0

Fax: 0211.38424-10

Email: poststelle@ldi.nrw.de

Disclosure to Third Parties

We do not disclose your personal data to third parties without your explicit and revocable consent at any time.

Exceptions to this are our service partners who require the transmission of data for order processing or for one of the purposes mentioned above (e.g., logistics partners for postal delivery and the credit institution responsible for payment processing). In these cases, the scope of the transmitted data is limited to the necessary minimum.

No further disclosure of your data to other third parties takes place.

If a disclosure to third parties occurs, we will agree and monitor the necessary data protection measures and compliance with legal data protection regulations with the

third party. In the case of required consent, we will inform you about who will receive your personal data.

International Data Transfers/Data Processing in Third Countries

If we transfer data to a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)) or if this occurs as part of using third-party services or disclosing or transmitting data to other persons, entities, or companies, this is always done in compliance with legal requirements.

There is an EU adequacy decision for the United Kingdom. The European Commission regularly reviews whether the level of data protection remains comparable to the requirements of the EU. For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which was recognized as a secure legal framework by an adequacy decision of the EU Commission on 10.07.2023. Additionally, we have concluded standard contractual clauses with the respective providers that comply with the EU Commission's requirements and establish contractual obligations to protect your data.

This dual protection ensures comprehensive protection of your data: The Data Privacy Framework (DPF) forms the primary protection level, while the standard contractual clauses serve as additional security. If changes occur within the DPF framework, the standard contractual clauses act as a reliable fallback option. This ensures that your data remains adequately protected even in the event of political or legal changes.

We inform you about our service partners, whether they are certified under the DPF and whether standard contractual clauses are in place. Further information on the DPF and a list of certified companies can be found at <https://www.dataprivacyframework.gov/>.

If we carry out data transfers to other third countries, the corresponding security measures apply, in particular standard contractual clauses, explicit consents, or legally required transfers. Information about third-country transfers and applicable adequacy decisions can be found at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de

Changes to This Privacy Notice

This privacy notice was created on 29.11.2022. We reserve the right to change this privacy notice at any time with effect for the future. The current version is directly accessible via our website. Please regularly inform yourself about the applicable privacy notice.

Privacy Notice Status: April 2026

