Privacy Policy

For Metaroom ® by Amrax

Updated August 2025

1. Preamble

The services ‘Metaroom Workspace’ (hereinafter ‘Workspace’), ‘Metaroom Scan App’ (hereinafter ‘App’), and the website www.amrax.ai (hereinafter ‘Website’) are provided by Synthetic Dimension GmbH (hereinafter ‘we’ or ‘us’) as the controller within the meaning of the applicable data protection law. When you use one of these services, we collect and/or process personal data about you. Personal data is any information relating to an identified or identifiable natural person. As the protection of your privacy is important to us, we would like to inform you below about which personal data we process when you use the services and how we handle this data. In addition, we will inform you about the legal basis for processing your data and, if processing is necessary to protect our legitimate interests, also about our legitimate interests. You can access this Privacy Policy at any time within the app under the menu item ‘Privacy Policy’.

2. Information about the processing of your data

Certain information is processed automatically as soon as you use the app or the Workspace. Below we have listed which personal data is processed and for what purpose.

2.1. Collected data

2.1.1 Collected data during download

When you download the app, certain information required to download and install the app is transmitted to the selected app store (e.g. Apple App Store). In particular, the username, email address, customer number of your account, time of download, payment information, and individual device ID are processed. This data is processed exclusively by the respective app store provider and is outside our sphere of influence, which is why we refer you to the data protection information of these providers in this regard.

2.1.2 Paid packages

We process the personal data provided to us (title, name, company name, contact persons, e-mail address, telephone number, billing and delivery address, billing and payment data and information about orders) for the conclusion, execution or termination of a contract with you. Without the personal data you provide when ordering or contacting us, we cannot conclude a

contract with you. We therefore process this data to fulfil contractual obligations or to carry out pre-contractual measures in accordance with Art. 6 (1) lit b GDPR.

We are also authorized, insofar as this is necessary for debt collection purposes or to enforce our claims arising from the contractual relationship, to transmit master data and personal data that you have provided to us, in any case (company) name, address, details of late payment and outstanding balance to lawyers and debt collection agencies. The personal data will be stored by us for as long as is necessary to fulfil the purpose of the data processing and, insofar as a corresponding legal obligation exists or there are outstanding legal claims from a legal relationship relating to the data that require longer storage.

Your data will be stored for seven years to fulfil retention obligations under company, VAT and tax law. In addition, your data will be stored for as long as is necessary to enforce legal claims.

2.1.3. Data collected during use

As part of your use of the app and the Workspace, we automatically collect and process certain data that is required for use or to improve usability. This data processing is justified by the fact that (1) the processing is necessary for the fulfilment of the contract between you as the data subject and us in accordance with Art. 6 (1) lit b GDPR for the use of the app or (2) we have a legitimate interest in ensuring the functionality and trouble-free operation of the app and in being able to offer a service in line with the market and our interests in accordance with Art. 6 (1) lit f GDPR.

When you create a personalized account, you provide us with personal information that includes your full name, email address and password. This personal account information is necessary to identify you as a user and to grant you access to our services. The personalized account allows you to access the data you have created in the app on another device or in the Workspace. This data is processed and used to provide the service. This data is processed based on our existing overriding legitimate interests in accordance with Art. 6 (1) lit f GDPR and for the implementation of pre-contractual measures or fulfilment of the contract in accordance with Art. 6 (1) lit b GDPR. We cannot process your registration for a personalized account without your data. The data will be stored for as long as you have a customer account with us. You can delete your customer account at any time.

We also use your name and email address to inform you about new similar products and features. In this respect, the data processing is based on our legitimate interest in personalized direct advertising in accordance with Art. 6 (1) lit f GDPR in conjunction with § 174 (4) of the telecommunications act, TKG 2021. If you have initially expressly objected to the use of your e-mail address for this purpose, we will not send you any e-mails. You are entitled to object to the use of your email address for the aforementioned advertising purpose at any time with effect for the future by sending us a message. Once we have received your objection, we will immediately stop using your email address for this purpose.

During the scan with the app, we collect and transmit data obtained from visual sensors (cameras) and the on-board processing of the device for the fulfilment of contractual obligations in accordance with Art. 6 (1) lit b GDPR. This includes sequences of images, depth maps, 3D point clouds and location information. This data may contain your personal information, such as details about your room and the items in the room. To protect your privacy, image data of people is recognized by our software to make them unrecognizable. However, we would like to point out that recognition does not offer 100 per cent security and we generally recommend that you do not record people.

When using the Workspace, we do not collect any further data using visual sensor technology. Adjustments made to the model are saved to ensure the expected functionality, which results in a change or enrichment of the previously recorded and processed data. The data can also be (partially) deleted in this way.

2.1.4. Cookies

At Metaroom Workspace, we use technically necessary cookies in accordance with Art. 6 (1) lit f GDPR in conjunction with § 165 (3) TKG 2021 (telecommunication act) to ensure the basic functions of the site. The user's express consent is not required for these cookies.

We use cookies to improve the operation of our website. Cookies are small text files that can be stored on your computer when you visit a website. Cookies are generally used to provide users with additional functions on a website. You can adjust your cookie settings at any time via our cookie banner.

Functionality of the website: When you visit our website, the personal data that your browser transmits to our servers and that is technically necessary to display the website to you and to ensure its stability and security is collected (Art. 6 (1) lit f GDPR in conjunction with § 165 (3) TKG 2021). This supports the traceability of errors and sustainable troubleshooting. In addition, this serves to prevent and remedy illegal use of the website content and to improve the quality of the website. The IP address is only analyzed in the event of attacks on our network infrastructure. The data is automatically deleted as soon as it is no longer required for our recording purposes, but at the latest after 30 days.

The following data is recorded: IP address of the requesting device, country and city of the visitor, language setting of the visitor, date and time of access, operating system, device used, browser and add-ons used, files downloaded, videos played, banners clicked on, duration of the visit, website from which access was made, subpages accessed;

Web analysis: We use analysis and performance cookies as well as marketing and advertising cookies to statistically evaluate visits to the website, in particular to analyze the use of our website. If individual pages of our website are accessed, the following data is stored: the website accessed, the website from which the user accessed the website (referrer), the subpages accessed from the website accessed, the time spent on the website, the frequency with which

the website is accessed, the search terms, the date and time (including for your own time zone), the resolution, files clicked on and downloaded, links clicked on to external domains, browser-specific data (which browser, language);

This data is only processed on the basis of your consent in accordance with Art. 6 (1) lit a GDPR in conjunction with § 165 (3) TKG 2021, which you have expressly given us based on the cookie settings. You can revoke this consent at any time, but this revocation does not affect the legality of the data processing carried out up to that point.

Cookie settings: When you visit our website for the first time, a cookie banner appears informing you about the use of cookies and giving you the opportunity to adjust your cookie settings. You can choose which types of cookies you want to allow. Your selection will be saved and you can change or adjust these settings at any time via the cookie banner.

Managing cookies: In addition to the settings in the cookie banner, you can also adjust your cookie settings in your browser settings and prevent the acceptance of cookies in whole or in part. Please note that disabling cookies may limit the functionality of our website.

2.2 External services

Cloud data processing using Amazon AWS

We use Amazon Web Services to process data on our behalf as follows: AWS S3 (AWS storage service) is used to store personal room scans (including time codes in Europe, zone eu-west-1). Other AWS services process user data in technical operation without persisting it (AWS EC2, AWS Fargate, AWS Lambda):

We expressly point out that your data may be processed in the USA (third country). We have concluded an order processing contract with AWS that contains EU standard contractual clauses for the use of Amazon Web Services. Through this contract, Amazon assures that the company processes the data in accordance with the GDPR and guarantees the protection of the rights of the data subject. There is currently a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out based on Art. 45 (1) GDPR in conjunction with the EU-US Data Privacy Framework. AWS is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list

Data-driven optimization using Google Analytics

We also use Google Analytics for Firebase and Firebase Crashlytics (hereinafter referred to as Google Firebase) to analyze user behavior and to ensure the stability and continuous improvement of the app. The provider is Google Inc. based at 1600 Amphitheater Parkway, Mountain View, CA 94043, USA. Firebase contains various functions with which we can analyze

in-app behavior. For example, we can analyze screen views and button clicks. We can also determine which functions within our app are used frequently or rarely.

Anonymous information on the frequency of use is used to evaluate the general acceptance of the app and analyze whether further developments of the app have a positive impact. Anonymous information on session/dwell time is used to identify errors in the usability of the app and to optimize content accordingly. Anonymous screen sequences or the processes involved in using the app help us to better understand users' use cases and goals and to speed up frequently used processes in the app. Demographic data is used to better understand our target group. For these purposes, Google Firebase stores the number and duration of sessions, operating systems, device models, region and a range of other data. You can find a detailed overview of the data collected by Firebase at the following links: support.google.com/firebase/answer/6318039, https://firebase.google.com/support/privacy/#examples_of_end-user_personal_data_processed_by_firebase

Firebase Crashlytics is used to monitor and promptly fix app errors. When the app crashes, certain information about the crash such as time of crash, device type, operating system and other technical details are sent from your mobile device to Crashlytics. These crash reports are stored anonymously, i.e. they do not contain an IP address or other personally identifiable information.

The use of Google Firebase may require the transfer of your personal data to the USA. There is currently a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out based on Art. 45 (1) GDPR in conjunction with the EU-US Data Privacy Framework. Google Inc. is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list

The storage period for the data collected can be found in the provider's privacy policy. Google Firebase is used to optimize this app and to improve our services. This constitutes a legitimate interest within the meaning of Art. 6 (1) lit f GDPR. However, the processing of data for analysis purposes is only carried out based on your consent in accordance with Art. 6 (1) lit b GDPR in conjunction with § 165(3) TKG 2021. You can find more information about Google Firebase at the following links: https://firebase.google.com/, https://firebase.google.com/terms/crashlytics/, https://firebase.google.com/support/privacy/

Customer relationship management using Hubspot

We use services from Hubspot, a customer relationship management registration and marketing automation system from the provider Hubspot Inc. (25 First Street, 2nd Floor, Cambridge, MA 02141, USA) with offices in Ireland (Ground Floor, Two Dockland Central, Guild Street, Dublin 1) and Germany (Am Postbahnhof 17, 10243 Berlin). We use these services for contact

management, email marketing (newsletters, automated mailings), provision of product-related information such as new functions or updates/upgrades, reporting (e.g. traffic sources, hits, etc.), landing pages and contact forms. If you create an account to use our products or otherwise provide us with contact information and other demographic information (e.g. via the contact form on our websites), we may share this information, and the content accessed on our websites or in our products with Hubspot. Hubspot's services help us to contact visitors to our websites and interested parties and users of our products and, for example, to answer their enquiries and determine which of our company's services are of interest to them. In addition, these services enable us to work more efficiently with our products and thus generally help to improve usability and service quality.

The legal basis for this processing is your express consent (Art. 6 (1) lit a GDPR) and the protection of our legitimate interests (Art. 6 (1) lit f GDPR), namely the improvement of the user experience and service quality (e.g. efficient and fast processing of enquiries). Hubspot is a provider based in the USA. We have therefore concluded a contract with HubSpot with standard contractual clauses within the meaning of Art. 46 (2) GDPR, in which HubSpot undertakes to process user data only in accordance with our instructions and to comply with the EU data protection level. There is currently also a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out based on Art. 45. (1) GDPR in conjunction with the EU-US Data Privacy Framework. Hubspot Inc. is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list

Further information about Hubspot can be found at the following links: https://legal.hubspot.com/de/dpa, https://legal.hubspot.com/de/privacy-policy

Payment service provider Stripe

We offer the option of processing the payment transaction via the payment service provider Stripe, 510 Townsend St., San Francisco, CA 94103. This corresponds to our legitimate interest in providing an efficient and secure payment method (Art. 6 (1) lit f GDPR). Without the transmission of your personal data (name, address, bank details, account number or credit card number, payment reference), we cannot offer payment via Stripe. As the controller under data protection law, Stripe uses your transmitted data to fulfil contractual obligations and process the payment transaction. This serves the fulfilment of the contract (pursuant to Art. 6 (1) lit b GDPR). Please also note its General Terms and Conditions in the context of payment processing. Stripe has implemented the necessary compliance measures for international data transfers. These apply to all activities in which Stripe processes personal data of natural persons in the EU. These measures are based on the EU standard contractual clauses. There is currently also a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out based on Art. 45 (1) GDPR

in conjunction with the EU-US Data Privacy Framework. Stripe is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list

Further information on objection and removal options with respect to Stripe can be found at: https://stripe.com/privacy-center/legal. Your data will be stored by us until payment processing has been completed. This also includes the period required for the processing of refunds, receivables management and fraud prevention (see also section 2.1.2. Paid packages)

Managing contact data using Zoho

To store and efficiently manage our contact data, we also use the Zoho CRM customer relationship management system from Zoho Corporation, 4141 Hacienda Drive Pleasanton, CA 94588, USA. Zoho is a provider based in the USA. We have concluded a contract with Zoho with standard contractual clauses within the meaning of Art. 46 (2) GDPR, in which Zoho undertakes to process the contact data only in accordance with our instructions and to comply with the EU data protection level. Further information can be found on the Zoho website (https://www.zoho.com/gdpr.html). The legal basis for the processing of contact data is the protection of our legitimate interests (Art. 6 (1) lit f GDPR), namely the establishment of a business relationship and the maintenance of our business contacts (CRM) as well as the fulfilment of contractual obligations in accordance with Art. 6 (1) lit b GDPR.

Sales organization using SalesLoft

We also use various tools to process the data stored in our CRM systems. These include the SalesLoft sales platform, which we use to improve the organization of our sales processes. SalesLoft accesses some of the customer data contained in our CRM systems (contact information and company information) and combines this with information about the interactions that have taken place with us (e.g. telephone calls, communication via email and/or social networks). This information helps us to coordinate our sales activities centrally and to communicate with our customers authentically and always up to date. SalesLoft is a provider based in the USA. We have therefore concluded a contract with SalesLoft with standard contractual clauses within the meaning of Art. 46 (2) GDPR, in which SalesLoft undertakes to process user data only in accordance with our instructions and to comply with the EU level of data protection. There is currently also a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out based on Art. 45 (1) GDPR in conjunction with the EU-US Data Privacy Framework. SalesLoft is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list. The legal basis for this processing is the protection of our legitimate interests (Art. 6 (1) lit f GDPR), namely the ongoing optimization of our sales processes.

Geolocation using OpenStreetMap and Google Maps

We use the OpenStreetMap service to derive the address of buildings based on GPS data. The IP address and GPS data are passed on to OpenStreetMap. The GPS data is only passed on in order to determine the exact address of buildings and to display the location information accordingly. This enables us to provide you with precise information about your surroundings and the addresses you are looking for. Your IP address and GPS data are processed on the basis of your consent in accordance with Art. 6 (1) lit a GDPR, which you give us by using our services and accepting this privacy policy.

Finally, in our app you have the option of viewing the location of buildings via a link to Google Maps. The link to Google Maps allows you to visualize the location of buildings and get directions. If you use the link to Google Maps, you will be redirected to the Google Maps website. Your IP address and the location data (GPS data) of the scan will be transmitted to Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. In the course of using Google Maps, your data may be transferred to the USA (third country). There is currently a decision by the European Commission in which the level of data protection for certified companies in the USA is declared appropriate and any data processing is carried out on the basis of Art. 45 (1) GDPR in conjunction with the EU-US Data Privacy Framework. Google LLC is a certified company. The list of certified companies is available at https://www.dataprivacyframework.gov/list

Google Maps processes this data in accordance with its own privacy policy, which you can view here: https://policies.google.com/. The transfer and processing of your data is based on your consent in accordance with Art. 6 (1) lit a GDPR, which you give us by using our services and accepting this privacy policy.

3. Period of data storage

We delete or anonymize your personal data as soon as it is no longer required for the purposes for which we collected or used it in accordance with the above paragraphs. As a rule, we store your personal data for the duration of the usage or contractual relationship via the app plus a period of 14 days, unless this data is required for longer for criminal prosecution or to secure, assert or enforce legal claims.

This does not affect special information in this privacy policy or legal requirements for the retention and deletion of personal data, in particular data that we must retain for seven years for reasons of company, VAT and tax law.

4. Obligation to provide data

There is no legal obligation to provide data. However, our services and some functions or our website cannot be used without the provision of personal data. Furthermore, we cannot enter into or fulfil a contract with you without your data. However, you are not obliged to give your consent to data processing with regard to data that is not relevant or legally required for the fulfilment of the contract.

5. Your rights as a data subject

You can request information about your data processed by us (Art. 15 GDPR). If your data is not (or no longer) correct, you can request that it be corrected (Art. 16 GDPR) If your data is incomplete, you can request that it be completed. You also have the right to erasure your data (Art. 17 GDPR), to restriction of data processing (Art. 18 GDPR) and to data portability (Art. 20 GDPR).

If data is processed based on legitimate interests, you have the right to object. You can also withdraw your consent at any time. If you have any questions or concerns regarding the processing of your personal data, please contact us:

Synthetic Dimension
Urstein Süd 19/1/5,
5412 Puch/Hallein
Austria

Phone: +43 664 9957763
E-mail: office@amrax.ai

If you have any questions about data protection, please contact our data protection officer by email at data.privacy@amrax.ai.

In addition, you have the right to complain to the Austrian Data Protection Authority (Barichgasse 40-42, 1030 Vienna) via dsb@dsb.gv.at if you think that the processing of your personal data is not lawful.