Privacy Policy

Contents

Scope and Application . . . 3
Part A: End-User Data Processing . . . 3
A.1 Which data are collected from end users? . . . 3
A.3 How is end-user data used? . . . 3
A.4 Processing of personal data (end users) . . . 4
A.5 Transfer of end-user personal data to third parties . . . 4
A.6 Possible risks (end-user data) . . . 5
A.7 Data retention (end-user data) . . . 5
A.8 Rights of end users in connection with personal data . . . 6
Part B: Customer Data Processing . . . 6
B.1 Which customer data are collected? . . . 6
B.2 Automated probe measurements . . . 6
B.3 How is customer data used? . . . 7
B.4 AI-assisted analysis features . . . 7
B.5 Customer data retention . . . 7
Part C: Infrastructure and Subprocessors . . . 8
C.1 Subprocessors . . . 8
C.2 Data transfers outside the European Economic Area . . . 9
Part D: Software Telemetry . . . 9
D.1 What is telemetry data? . . . 9
D.2 Which telemetry data are collected? . . . 9
D.3 How is telemetry data used? . . . 9
D.4 Processing of personal data (telemetry) . . . 10
D.5 Telemetry data retention . . . 10
D.6 Telemetry and consent . . . 11
D.7 Rights of users in connection with telemetry data . . . 11
Part E: General Provisions . . . 11
E.1 Data controller . . . 11
E.2 Contact . . . 12
E.3 Complaints . . . 12

Scope and Application

1. This Privacy Policy describes how AVEQ GmbH (“we”, “us”, “our”) collects, uses, and shares data in connection with the Surfmeter software products and online services.
2. This policy applies to:
    1. **End users** whose data is collected through Surfmeter software (e.g., users of apps with Surfmeter Player SDK integrated)
    2. **Customers** (Licensees) who use Surfmeter products and the Online Service
3. The applicability of specific sections depends on how the Software is deployed and used.

Part A: End-User Data Processing

This part applies to the following products when used to collect data from end users: Surfmeter Player SDK.

A.1 Which data are collected from end users?

1. The data collected with this software includes the following data points when a video is played in software connected to the Surfmeter Player SDK:
    1. Video playback events (such as play, pause, quality changes, load times, fast forward, full screen change, and player debug information)
    2. Video metadata (such as video ID, title, likes, dislikes, number of comments, and categories)
    3. Advertisement insertion times
    4. Clicks on ad skip buttons
    5. Web page performance data (such as loading times via the Navigation Timing API and Javascript events), scrolling behavior of the user
    6. Status of login to a website
    7. Type of account (e.g., Premium or Normal)
    8. Client UUID (a unique identifier for the device)
    9. Rough location (city and country) and Internet service provider as determined by the IP address
    10. Exact location based on browser geolocation data (only with the user’s consent)
    11. Device and browser information (including operating system and version, browser type and version, screen resolution, window resolution, and user agent string), and for mobile devices, network information (such as WLAN SSID, mobile network operator, Cell ID, and signal strength), if applicable permissions have been granted.

A.3 How is end-user data used?

1. The data is collected, processed, and stored for the primary purpose of analyzing video streaming or web browsing quality in relation to the network connection.
2. In addition, the data collected by AVEQ GmbH employees and subcontracted companies may be used at any time, without limitation, for the following purposes:
    1. IT administration and security (such as checking for authorized or unauthorized access)

2. Maintenance and optimization of the software
3. Improvement of the offered services
4. Research and investigations
5. Dispute resolution and regulatory compliance

3. For the following purposes, the data may only be used with the prior consent of the data subject:
    1. Advertising and marketing
    2. Scientific publications

A.4 Processing of personal data (end users)

1. The following personal data are processed in the context of software use only with the consent of the user:
    1. **Client UUID and device IDs.** The purpose of processing this data is to enable history for users, to identify related tests (especially in connection with misuse or malfunctions), and to allow the user to exercise their rights according to the General Data Protection Regulation (GDPR).
    2. **IP address.** The purpose of processing this data is to technically enable the determination of the performance data of an Internet provider, to ensure the full range of functions, to allocate data to Internet providers, place names, or federal states, and to detect misuse and malfunctions.
    3. **Geolocation data.** The purpose of processing this data is to technically enable the determination of the performance data of an Internet provider in certain locations and regions, and to detect misuse and malfunctions.
2. The personal data are processed by AVEQ GmbH.

A.5 Transfer of end-user personal data to third parties

1. The personal data may be transmitted to the following recipients, including to third countries:
    1. **Client UUID.** This identifier may be transmitted to third-party providers (such as Internet service providers) in pseudonymized form for the purposes of quality determination and traceability.
    2. **IP address.** To determine the Internet service provider (ISP) or routing information (AS) of an IP address, this data is sent to Kloudend, Inc. (https://ipapi.co/). The privacy policy of Kloudend, Inc. is available at: https://ipapi.co/privacy/. Only the IP address is transferred, which does not allow any conclusions to be drawn about the other personal data.
    3. **Geolocation data.** To determine place names and regions, the geolocation data of the browser may be sent to one of the following providers:
        1. Unwired Labs LocationIQ (https://locationiq.com/). The privacy policy of Unwired Labs LocationIQ is available at: https://locationiq.com/privacy.
        2. OpenStreetMap Foundation (https://osmfoundation.org/). The privacy policy of the OpenStreetMap Foundation is available at: https://wiki.osmfoundation.org/wiki/Privacy_Policy.
        3. Geoapify (https://www.geoapify.com/). The privacy policy of Geoapify is available at: https://www.geoapify.com/privacy-policy.
        4. Only the geolocation data is transferred, which does not allow any conclusions to be drawn about the other personal data. Rounded geolocation data may also be sent to third parties (such as Internet service providers) together with pseudonymized identifiers.

4. **Measurement data for AI-assisted analysis.** Measurement data may be sent to the following AI service providers for the purpose of AI-assisted analysis:
    1. Google LLC (Gemini API). The terms of service are available at: https://ai.google.dev/gemini-api/terms. The data processing terms are available at: https://business.safety.google/processorterms/.
    2. OpenAI, LLC. The privacy policy is available at: https://openai.com/enterprise-privacy/.
    3. Anthropic, PBC. The privacy policy is available at: https://platform.claude.com/docs/en/legal-center/privacy.
    4. When enabled by the Licensee, AVEQ may perform automated AI analyses (such as anomaly detection, pattern recognition, or quality trend analysis) as part of the service. This automated processing is covered by the service agreement with the Licensee and does not require separate per-use consent.
2. **Legal basis for transfers.** The data transmission to these third parties is based on adequacy decisions of the European Commission in accordance with Article 45 of the General Data Protection Regulation (GDPR), or with the prior consent of the user according to Article 49(1)(a) of the General Data Protection Regulation (GDPR). In the latter case, the data subject has expressly consented to the proposed data transfer after being informed about the possible risks of such data transfers without an adequacy decision and without suitable guarantees.

A.6 Possible risks (end-user data)

1. A possible risk in data transmission is that the IP address of the user is transmitted to third parties, and thus conclusions about the use of this software may be drawn. However, the processing companies cannot link any other transmitted data to the Client UUID.
2. Another possible risk is that the geolocation data of the user is transmitted to third parties, and thus conclusions about the location of the user may be drawn. The IP address and the geolocation data cannot be linked to each other by the receiving third parties.
3. When AI service providers are used, the data is processed on servers that may be located outside the European Economic Area. Users should review the privacy policies of the AI providers to understand how their data may be used. AI providers may use data according to their respective terms of service.

A.7 Data retention (end-user data)

1. The following personal data is stored as follows:
    1. **Client UUID.** This identifier is deleted when the service that uses this software is finally discontinued.
    2. **IP address.** The IP address is stored temporarily, processed, and anonymized immediately after the determination of the Internet provider. For IPv4 addresses, only the first three bytes are stored. For IPv6 addresses, only the first four bytes are stored. The full IP address is stored for a maximum of one hour for caching purposes, but not in connection with the Client UUID. The anonymized IP address is deleted when the service that uses this software is finally discontinued. For the purpose of preventing improper use, the full IP address is also temporarily stored in web server logs and finally deleted after a reasonable time.
    3. **Geolocation data.** Geolocation data is deleted when the service that uses this software is finally discontinued.

A.8 Rights of end users in connection with personal data

1. With the appropriate Client UUID, the user has the following rights under the General Data Protection Regulation (GDPR):
    1. The right to be informed about the collection and use of their personal data.
    2. The right of access to their personal data.
    3. The right to rectification of inaccurate personal data.
    4. The right to erasure of their personal data (the “right to be forgotten”).
    5. The right to restrict processing of their personal data.
    6. The right to data portability.
    7. The right to object to processing of their personal data.
    8. Rights in relation to automated decision making and profiling.
2. Please note that it is not possible to fulfill a request under the GDPR without disclosing the Client UUID.

Part B: Customer Data Processing

This part applies to all Surfmeter products and the Online Service when used by Licensees (customers).

B.1 Which customer data are collected?

1. When customers use the Software or Online Service, we collect the following categories of data:
    1. **Account information.** This includes the username, email address, and organization name provided during account creation.
    2. **Authentication data.** This includes login timestamps and session information necessary for secure access to the service.
    3. **Usage data.** This includes information about actions performed in the Online Service and feature usage patterns.
    4. **Configuration data.** This includes software settings and measurement configurations chosen by the customer.
    5. **Measurement data.** This includes the results from measurements performed with the Software.
2. It is important to note that measurement data may include end-user personal data (as described in Part A of this Privacy Policy) or may consist solely of automated probe data with no personal data, depending on how the Software is deployed by the customer.

B.2 Automated probe measurements

1. When the Software is used solely for automated measurements from probes or test infrastructure (without end-user involvement), no end-user personal data is collected. In such cases, Part A of this Privacy Policy does not apply, and the data collected consists of technical measurement results only.

B.3 How is customer data used?

1. Customer data is used for the following purposes:
    1. Providing and maintaining the Software and Online Service, including ensuring the proper functioning of all features and capabilities.
    2. Customer support and communication, including responding to inquiries and providing technical assistance.
    3. Service improvement and optimization, including analyzing usage patterns to enhance the user experience and functionality of the Software.
    4. Compliance with legal obligations, including responding to lawful requests from authorities and maintaining records as required by applicable laws.
    5. Security and fraud prevention, including detecting and preventing unauthorized access or misuse of the service.

B.4 AI-assisted analysis features

1. The Online Service offers AI-assisted analysis features for analyzing measurement data. These features fall into two categories:
    1. **User-Initiated AI Features.** These are interactive AI features (such as chat-based queries, data comparison, or natural language analysis) that customers or authorized users explicitly invoke. When using these features, the following applies:
        1. Users must accept the AI feature terms before first use. This ensures that users understand how their data will be processed and by which providers.
        2. Measurement data selected by the user is sent to AI providers for processing. Only the data specifically selected or referenced by the user in their query is transmitted.
        3. When measurement data includes end-user personal data, customers are responsible for ensuring that an appropriate legal basis exists for such processing. This may include obtaining consent from end users or ensuring that another lawful basis under GDPR applies.
    2. **Automated AI Processing.** AVEQ may use AI services to perform automated analyses on measurement data as part of the Online Service. This includes functionality such as anomaly detection, pattern recognition, or quality trend analysis. For automated AI processing, the following applies:
        1. Such processing is performed by AVEQ as part of the service delivery and improvement. It is an integral part of the service offering.
        2. Automated AI processing may be enabled or disabled by customers via service configuration or upon agreement with AVEQ.
        3. Automated AI processing does not require per-use consent but is covered by the license agreement and the applicable Data Processing Agreement where the Licensee acts as data controller.
2. The AI service providers used for these features include Google (Gemini), OpenAI, and Anthropic. The specific provider used depends on the feature and configuration.

B.5 Customer data retention

1. Customer data is retained according to the following principles:

1. **Account data.** Account data is retained for the duration of the license agreement plus any legal retention periods required by applicable law.
2. **Measurement data.** Measurement data is retained as agreed in the license terms or deleted upon customer request.
3. **Usage logs.** Usage logs are retained for security purposes for a reasonable period, after which they are deleted or anonymized.

Part C: Infrastructure and Subprocessors

C.1 Subprocessors

1. AVEQ GmbH engages the following subprocessors to provide the Software and Online Service:
    1. **Infrastructure Subprocessors**
        1. Hetzner Online GmbH, located at Industriestr. 25, 91710 Gunzenhausen, Germany. Hetzner provides server hosting and data storage services. This subprocessor is engaged for all customers.
        2. Google Cloud Platform (Google LLC), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google Cloud Platform provides backup storage services in the EU region. This subprocessor is only engaged when the customer opts into cloud backup services.
    2. **Data Enrichment Subprocessors**
        1. Kloudend, Inc. (ipapi.co), located in the USA. Kloudend provides IP address to ISP and location lookup services. This subprocessor is engaged when end-user data is processed.
        2. Unwired Labs (LocationIQ), located in the USA. Unwired Labs provides reverse geocoding of coordinates. This subprocessor is engaged when end-user data is processed.
        3. OpenStreetMap Foundation, located at St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, United Kingdom. OpenStreetMap Foundation provides reverse geocoding of coordinates. This subprocessor is engaged when end-user data is processed.
        4. Geoapify GmbH, located in Germany. Geoapify provides reverse geocoding of coordinates. This subprocessor is engaged when end-user data is processed.
    3. **AI Service Providers**
        1. Google LLC (Gemini API), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google provides AI-assisted analysis of measurement data. This subprocessor is engaged for user-initiated AI features or automated AI processing.
        2. OpenAI, LLC, located at 3180 18th Street, San Francisco, CA 94110, USA. OpenAI provides AI-assisted analysis of measurement data. This subprocessor is engaged for user-initiated AI features or automated AI processing.
        3. Anthropic, PBC, located at 548 Market St, San Francisco, CA 94104, USA. Anthropic provides AI-assisted analysis of measurement data. This subprocessor is engaged for user-initiated AI features or automated AI processing.

C.2 Data transfers outside the European Economic Area

1. For transfers to subprocessors located outside the European Economic Area, we ensure that personal data is adequately protected through one of the following mechanisms:
    1. We rely on adequacy decisions of the European Commission where applicable, which confirm that the third country ensures an adequate level of data protection.
    2. We use EU Standard Contractual Clauses (SCCs) approved by the European Commission, which provide appropriate safeguards for the transfer of personal data.
    3. We obtain explicit consent from the data subject under Article 49(1)(a) of the GDPR, after informing them of the possible risks of such transfers.
2. Users are informed of potential risks before providing their consent to data transfers outside the EEA.

Part D: Software Telemetry

This part applies to all Surfmeter products that require registration or license verification.

D.1 What is telemetry data?

1. Telemetry data is technical information that is collected for the purposes of licensing, auditing, and software improvement. Telemetry data is distinct from measurement data (described in Part A) and customer account data (described in Part B).
2. In connection with the registration and use of the Software, telemetry data may be transmitted to AVEQ GmbH's servers at any time for processing.

D.2 Which telemetry data are collected?

1. The telemetry data collected includes the following data points when you install the software, register the software, or perform measurements with the software:
    1. **Client UUID.** This is a unique identifier for the device, which is generated at the time of registration.
    2. **Registration key.** This is the license key that is used to register the Software.
    3. **Registration timestamp.** This is the date and time when the Software was registered.
    4. **Usage statistics.** This includes the type and number of measurements performed by the Software.
    5. **IP address.** Only the first three octets of the IP address are stored. The last octet is truncated immediately upon collection to ensure anonymization.
    6. **Device information.** This includes information about the device used, such as the operating system and version, browser type and version (if applicable), screen resolution, and user agent string.

D.3 How is telemetry data used?

1. The telemetry data is collected, processed, and stored for the primary purpose of auditing, specifically to monitor the number of registrations and instances of the Software in operation.

2. In addition, the telemetry data collected by AVEQ GmbH employees and subcontracted companies may be used at any time, without limitation, for the following purposes:
    1. IT administration and security, including checking for authorized or unauthorized access to the Software.
    2. Detection of misuse and malfunctions, including identifying instances where the Software is being used in violation of the license terms or is not functioning correctly.
    3. Ensuring compliance with licensing terms, including verifying that the number of active installations does not exceed the licensed amount.
    4. Software improvement, including analyzing aggregate, anonymized usage patterns to improve the functionality and performance of the Software.
    5. Technical support, including diagnosing issues when troubleshooting assistance is requested by the Licensee.
    6. Dispute resolution and regulatory compliance, including supporting the resolution of licensing disputes and ensuring compliance with applicable laws and regulations.
3. AVEQ GmbH commits not to use the telemetry data for any other purposes, including sales or marketing purposes. AVEQ GmbH shall not disclose this data to third parties, except as mandated by legal requirements or as necessary for enforcing licensing agreement terms.

D.4 Processing of personal data (telemetry)

1. The following personal data are processed in the context of telemetry data collection only with the consent of the user:
    1. **Client UUID.** The purpose of processing this data is to enable identification of registered instances of the Software, to detect misuse or malfunctions, and to allow the user to exercise their rights according to the General Data Protection Regulation (GDPR).
    2. **IP address.** The purpose of processing this data is to detect misuse and malfunctions and to analyze the approximate geographic distribution of Software installations.
2. Both parties recognize that IP addresses can be considered personal data under the General Data Protection Regulation (GDPR) if they can be linked to an identifiable natural person. AVEQ GmbH is committed to treating all IP addresses with the same level of privacy protection, regardless of whether they are associated with natural persons or not. Accordingly, AVEQ GmbH will anonymize IP addresses by truncating the last octet immediately after recording the data.
3. The personal data are processed by AVEQ GmbH.

D.5 Telemetry data retention

1. Telemetry data (such as registration timestamps, usage statistics, and device information) is retained for the duration of the license agreement and for a period of up to thirty-six (36) months after its termination for audit and compliance purposes. After this period, all telemetry data will be permanently deleted or fully anonymized such that it no longer constitutes personal data.

D.6 Telemetry and consent

1. For commercial licenses, telemetry data processing is essential for the performance of the license agreement and for contract enforcement. Such processing is covered by the license agreement and does not require separate consent from the Licensee.
2. For research or evaluation licenses, the Licensee acknowledges that telemetry data processing is essential for the performance of the license agreement and for contract enforcement. By accepting the license agreement, the Licensee provides explicit consent to the telemetry data processing described in this section. The Licensee understands that without this consent, the Software cannot function and the license cannot be granted. The Licensee may withdraw this consent at any time, but such withdrawal will result in immediate termination of the license agreement and the Licensee's right to use the Software.

D.7 Rights of users in connection with telemetry data

1. With the appropriate Client UUID, the user has the following rights under the General Data Protection Regulation (GDPR):
    1. The right to be informed about the collection and use of their personal data.
    2. The right of access to their personal data.
    3. The right to rectification of inaccurate personal data.
    4. The right to erasure of their personal data (the "right to be forgotten").
    5. The right to restrict processing of their personal data.
    6. The right to data portability.
    7. The right to object to processing of their personal data.
    8. Rights in relation to automated decision making and profiling.
2. Please note that it is not possible to fulfill a request under the GDPR without disclosing the Client UUID.
3. For research or evaluation licenses, the Licensee acknowledges that exercising rights to object, erasure, restriction, or portability of telemetry data will result in immediate termination of the license agreement, as telemetry processing is a condition of the license grant.

Part E: General Provisions

E.1 Data controller

1. The entity responsible for the processing of personal data within the meaning of Article 4(7) of the General Data Protection Regulation (GDPR) is:

    AVEQ GmbH
    Habitzlgasse 4/30
    1210 Wien
    Austria

E.2 Contact

1. For privacy inquiries, please contact: privacy@aveq.info
2. The Data Protection Officer can be reached at: privacy@aveq.info

E.3 Complaints

1. You have the right to lodge a complaint with a supervisory authority, in particular in the EU Member State of your habitual residence, place of work, or place of the alleged infringement, if you consider that the processing of personal data relating to you infringes the General Data Protection Regulation (GDPR).

Version: 2.10
Date: 30.01.2026

AVEQ GmbH
Habitzlgasse 4/30
1210 Wien
Austria

https://aveq.info
hello@aveq.info