

Data Protection Objectives

Our employees, customers, suppliers and all other interested parties are our most valuable assets. We recognize that building a long-term business relationship with you depends to a large extent on trust. This trust begins with our commitment to respect and protect your privacy.

The principal legal rules governing our handling of confidential and personal data are the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) and, for access to information on terminal devices, the German Telecommunications Digital Services Data Protection Act (TDDDG).

- We shall be compliant with legal requirements.
- We shall not sell or buy confidential or personal data, even if this might be legal under certain conditions.
- We shall protect all confidential or personal data from unauthorized access by implementing state-of-the-art security measures.
- We shall only process personal data if required to fulfill a certain task and for a legitimate purpose.

To offer transparency about the data we store and process, this Privacy Statement, AP Sensing Terms of Sale & Purchasing as well as Employee information on Data Protection and Processing shall be made easily available for all parties with a legitimate interest.

All AP Sensing staff is requested to support these objectives in their daily work and follow the relevant procedures in place.

Clemens Pohl - Managing Director
Böblingen, Germany, May 2026

Privacy Policy

This Policy was last revised on August 25th, 2026.

AP Sensing GmbH, Herrenberger Str. 130, 71034 Böblingen, Germany, is the controller for the processing described in this Privacy Policy on apsensing.com. Where affiliated companies process personal data for their own purposes, they generally act as separate controllers and provide additional privacy information where required. This Privacy Policy explains how AP Sensing GmbH processes personal data online and offline and the rights available to you.

The processing of personal data is governed in particular by the GDPR, the BDSG and the TDDDG. This Privacy Policy describes the material processing activities connected with our website, forms and the business and marketing contacts described below.

You can generally use our website without directly providing your name. However, technically necessary connection data is processed when the website is accessed; additional data is collected only for the purposes and on the legal bases described below. Mandatory fields are identified in the relevant form. If required information is not provided, the requested service may not be available.

AP Sensing's Privacy Policy covers 10 main areas: Fundamentals, Choice and Revocation, Third-country Transfers, Access and Accuracy, Data Security, Storage and Retention Periods, Cookie Use, Website Services and Forms, Marketing Tools and Additional Information. These areas are described in detail below. Privacy practices may vary where local law requires. Comments or questions may be sent to privacy@apsensing.com.

Responsible in the legal sense of any privacy laws

AP Sensing GmbH

Managing Director: Clemens Pohl (CEO)

Herrenberger Str. 130

71034 Böblingen, Germany

Phone: +49 7031 309 6610

E-Mail: info@apsensing.com

Place of Incorporation: Böblingen -- Commercial Register Stuttgart: HRB 72 48 80

VAT ID: DE 256976415

Data Protection Officer:

Nicole Paredes
AP Sensing GmbH
Herrenberger Str. 130
71034 Böblingen, Germany
e-mail: privacy@apsensing.com

Data Protection Authority in Baden-Württemberg, Germany:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Heilbronner Straße 35, 70191 Stuttgart, Germany
Postal address: Postfach 10 29 32, 70025 Stuttgart, Germany
Phone: +49 711 61 55 41 – 0, e-mail: poststelle@lfdi.bwl.de

1 Fundamentals

What information we collect (Art. 5 et seq. GDPR)

During the course of your relationship with us, we may collect, process and use personal information to enable you to order products or services, download software updates, make requests, and register for customized communications programs. Personal data consists of all information related to an identified or identifiable natural person, means data that is an expression of a person's identity. We may collect such personal data as your name, contact and transaction information, payment data and IP address. To tailor our subsequent communications to you and improve our products and services, we may ask you to provide information regarding your personal or professional interests, demographics, experience with our products and contact preferences. Personal information may be required to determine access eligibility for certain restricted parts of our site. Data collected online may be combined with information provided offline. Following the requirements to avoid or to minimize any unnecessary data storage, we only collect data needed to reasonably run our business or to meet any legal requirements.

For individual services, such as use of applications, we may also collect information that is necessary to visit, use or navigate these services. This information may include device and usage information or location data. You will be informed separately within these services about the data collection and all relevant information.

What is the legal basis to process personal data

We process personal data only where a valid legal basis applies. Depending on the activity, this is in particular your consent (Art. 6(1)(a) GDPR), performance of a contract or steps taken at your request

before entering into a contract (Art. 6(1)(b) GDPR), compliance with a legal obligation (Art. 6(1)(c) GDPR), or our legitimate interests or those of a third party where your interests or fundamental rights do not override them (Art. 6(1)(f) GDPR).

How we collect personal data

We receive personal data primarily from you through our website, by e-mail, by telephone, in person or in the course of a business relationship. We may also receive professional contact data from lawful sources, such as trade-fair organizers, distribution partners or publicly accessible professional sources. Where data is not obtained directly from you, we provide the information required by Art. 14 GDPR unless an exemption applies.

AP Sensing uses cookies and other technologies such as web beacons, local shared objects, local storage, e-tags, and JavaScript, to collect online usage information. Please review AP Sensing's Cookie Policy under section 7 for more information.

Certain AP Sensing software or cloud-based applications collect software user information via an automatic data feed when connected to the internet. Specific information about which personal data is collected by a particular software product is available in the documentation associated with that product.

How we use the information (Art. 5 et seq. GDPR)

We use personal data in particular to respond to inquiries, take steps before and perform contracts, provide products, portals, downloads and support, maintain lawful business relationships, and comply with legal obligations. Advertising, newsletters, audience measurement and personalization are carried out only on the legal basis specified for the relevant activity and in accordance with your consent, preferences and objections.

E-mail opening and click measurement and website audience measurement are used only where described in this Privacy Policy and legally permissible. Non-essential analytics and marketing technologies are activated only after consent. Data is combined with CRM or lead information only where this is separately described and legally permissible.

Automated decision-making

As a rule, we do not make decisions based solely on automated processing in the activities described in this Privacy Policy that produce legal effects concerning you or similarly significantly affect you. Potential matches identified in sanctions screening are reviewed by a person before any decision is made. If an individual service differs, we will provide separate information.

With whom we share the information (Art. 28 GDPR)

AP Sensing does not sell or rent your personal data. We disclose data only where necessary for the described purposes and legally permitted, in particular to affiliated companies, contractually bound processors, independent controllers or public authorities. Processors are carefully selected, contractually bound and appropriately monitored.

Processors and service providers

We use carefully selected service providers to operate our business, website and IT processes. Depending on the service, these providers act as processors under Art. 28 GDPR or as independent controllers where required by law. Relevant categories include hosting and cloud providers; IT and communications providers; CRM and contact-management providers; marketing and newsletter providers; analytics, tracking and consent-management providers; security, backup and monitoring providers; and support and ticketing providers. Where a provider processes data outside the EEA, the safeguards described in section 3 apply. Information on the relevant recipients is available from privacy@apsensing.com.

What rights you have regarding your personal data (Art. 7, 12 et seq. GDPR)

Subject to the applicable legal requirements, you have rights of access, rectification, erasure, restriction of processing, data portability and objection. Where processing is based on consent, you may withdraw it at any time with effect for the future; this does not affect the lawfulness of processing before withdrawal. You may object to processing for direct marketing at any time. You also have the right to lodge a complaint with a data protection supervisory authority. To exercise your rights, contact privacy@apsensing.com.

2 Choice and revocation (Art. 7 GDPR)

You may withdraw consent at any time with effect for the future. Cookie choices can be changed through the cookie settings, and newsletters can be cancelled using the unsubscribe link. Where we rely on legitimate interests, you may object on grounds relating to your particular situation. An objection to direct marketing applies without any further balancing of interests.

3 Third Countries Transfer (Art. 44 et seq. GDPR)

We may transfer personal data to recipients outside the European Economic Area (EEA) only where the requirements of Arts. 44 et seq. GDPR are met. Depending on the recipient, this may be based on an adequacy decision, a valid certification under the EU-US Data Privacy Framework, or appropriate safeguards such as the EU Standard Contractual Clauses, together with supplementary measures where required. Information about recipients and safeguards is available from privacy@apsensing.com.

4 Access and Accuracy (Art. 5, 16 GDPR)

AP Sensing strives to keep your personal information accurate. We will provide you with access to your personal information, including making every effort to provide you with online access to your registration data so that you may review, update or correct your information at the AP Sensing site where it was submitted. To protect your privacy and security, we will also take reasonable steps to verify your identity before granting you access or enabling you to make corrections. If you cannot access your information on the web page, please telephone AP Sensing for assistance, or send your request to privacy@apsensing.com.

5 Data Security (Arts. 25 and 32 GDPR)

As an ISO 27001-certified company, AP Sensing implements appropriate technical and organizational measures under Arts. 25 and 32 GDPR to provide a level of security appropriate to the risk. These measures include access and authorization controls, encryption in transit, confidentiality obligations, backups and regular security reviews. Absolute security of electronic communications cannot be guaranteed; unencrypted e-mail in particular may involve risks.

6 Storage and retention periods (Art. 5 GDPR)

We retain personal data only for as long as required for the relevant purposes and legal bases. Relevant criteria include the duration of an inquiry, consent, contract or business relationship, the lifecycle of our products, statutory retention and limitation periods, and the establishment, exercise or defence of legal claims. Where required for product, project, support or traceability purposes, certain customer, supplier, order and project data may be retained for up to 30 years after the contractual relationship ends or the last order is received; ordinary contact data is not retained for the entire period merely for that reason.

When the purpose ceases and applicable periods expire, we delete or anonymize the data. Where immediate deletion from backups is technically impossible, the data is isolated from further operational use until scheduled overwriting. Specific periods for website, form and marketing processing are stated in the relevant sections below.

7 Cookies Usage

Cookies and similar technologies may be necessary to provide the website, remember your choices, protect forms or measure website use. Necessary technologies are used only to the extent required. Analytics, marketing and external-media functions are activated only after you have consented through our consent-management tool.

You may reject non-essential technologies without affecting the basic use of the website; individual optional features, such as embedded media, may then be unavailable. You can change your choice at any time through the cookie settings.

For non-essential technologies, storing information on or accessing information from your terminal device is based on consent under section 25(1) TDDDG. Strictly necessary technologies fall under the exemption in section 25(2) TDDDG. Any subsequent processing of personal data additionally requires the GDPR legal basis stated for the relevant service.

Consent Management Tool: CookieHub

We use CookieHub to manage and document your cookie choices. Processing is necessary to comply with our accountability obligations and for legally compliant, user-friendly consent management (Art. 6(1)(c) and (f) GDPR). Strictly necessary storage and retrieval of your choice is based on section 25(2) TDDDG. Your consent to optional technologies is the legal basis for activating those technologies and the subsequent data processing.

- a unique string of characters that is stored in a CookieHub cookie in your browser along with the cookie category settings. This token can be requested by you to find the entry from the consent log and demonstrate your consent choices.
- the full URL displayed by you when the cookie settings were configured in the CookieHub widget
- a reference to the version of the widget that was displayed at the time you gave consent
- your anonymized IP address, with the last part of the IP address replaced by a 0 to avoid the risk of identifying personal data
- the registered country code for the anonymized IP address block
- your agent string, which usually contains browser and operating system information
- the date and time of your consent

When CookieHub is used, consent and technical data collected through our website is transmitted to CookieHub ehf., Hafnargata 51-55, 230 Reykjanesbaer, Iceland, acting as our processor.

CookieHub stores your choice on your terminal device and in a consent log so that it can be respected on later visits and demonstrated. Consent-log data is retained only for as long as necessary to document and demonstrate consent choices and to meet applicable accountability requirements. You may change your choice at any time through the cookie settings.

Reviewing Cookie settings

When accessing our website for the first time or afterwards by adjusting the Consent Management Tool, you can review the cookies settings, decline cookies completely or withdraw afterwards your previously given consent to specific cookies only.

Bot protection: Friendly Captcha

To protect our forms and double-opt-in processes from automated submissions, we use Friendly Captcha, provided by Friendly Captcha GmbH, Am Anger 3-5, 82237 Wörthsee, Germany, acting as our processor. Technical connection, environment, interaction and functional data is processed; according to the provider, the IP address is anonymized by one-way hashing before storage. The legal basis is our legitimate interest in the security and functionality of our forms (Art. 6(1)(f) GDPR). Where strictly necessary information is stored on or read from the terminal device, section 25(2) TDDDG applies. Further information: <https://friendlycaptcha.com/legal/privacy/>.

8 Website Services and Forms

Customer and partner portal

If you create a customer or partner account, we process in particular the contact name, e-mail address, company, product serial number, login credentials and, optionally, company address and telephone number. Processing is necessary to set up and administer the account and provide firmware, updates and other requested services (Art. 6(1)(b) GDPR; additionally Art. 6(1)(f) GDPR for secure and efficient portal operation). Accounts are maintained during the active business relationship and reviewed at least annually for continuing authorization. When authorization ends, access is deactivated immediately and account data is generally deleted within 30 days and no later than three months, unless another legal basis requires continued retention.

Download and contact forms

If you request product information, operating instructions or other materials through our website, we process the data entered in the form. Mandatory fields are salutation, first and last name, country, e-mail address, company and company website; title is optional. The data is transmitted through SULU and processed in Microsoft 365/Outlook and the protected SharePoint location. To submit the request and access the download, you must actively consent to the processing of these data for providing the requested information and for contacting you in connection with your request. We use the data to provide the requested documents and handle the specific inquiry. The legal basis is your consent for this purpose (Art. 6(1)(a) GDPR) or, where the inquiry concerns specific pre-contractual steps or an existing contractual relationship, Art. 6(1)(b) GDPR.

Based on your consent, Marketing or Sales may contact you in connection with the requested materials and related products. Such follow-up contact is limited to no more than two contacts. You may withdraw your consent at any time with effect for the future.

Data collected through download and contact forms is retained for as long as necessary to process the request and any resulting business contact. It is then deleted or anonymized in accordance with our documented retention periods, unless statutory retention obligations, limitation periods or another legal basis require longer retention.

Newsletter Registration

If you register for our newsletter, we process your e-mail address and, where provided, your salutation, name, company, country and areas of interest. Newsletter distribution is activated only after you actively confirm the subscription link in the confirmation e-mail (double opt-in). The legal basis is your consent under Art. 6(1)(a) GDPR.

We use the data to send information about AP Sensing products, services, events, technical developments and company news. We also process newsletter opening and click data to measure newsletter performance and improve our communications. You may withdraw your consent at any time with effect for the future by using the unsubscribe link or contacting privacy@apsensing.com. Newsletter distribution stops following withdrawal. A minimal suppression and evidence record may be retained where necessary to document the withdrawal and comply with applicable legal requirements.

9 Marketing Tools

We use the marketing and analytics tools described below only for the stated purposes. Non-essential tracking and external-media functions are activated only after consent. Depending on the provider, processing may take place outside the EEA, particularly in the United States; the transfer mechanisms described in section 3 apply.

Newsletter

For newsletter distribution, we use Mailchimp, a service of The Rocket Science Group LLC d/b/a Mailchimp, United States (an Intuit company). The data processed includes e-mail address, name, company, country, interests, consent records and opening and click data. Opening and click tracking is enabled to measure newsletter performance and improve our communications. Mailchimp acts as our processor for newsletter distribution. The applicable data-processing agreement is in place. Transfers to the United States are covered by the EU-US Data Privacy Framework and, where applicable, the EU Standard Contractual Clauses. Further information: <https://mailchimp.com/legal/privacy/>.

Customer and brand surveys

We may invite customers and partners by e-mail to customer or brand surveys and process responses in Mailchimp or our CRM. The legal basis is generally our legitimate interest in improving our products and services (Art. 6(1)(f) GDPR); where the invitation or analysis requires consent, Art. 6(1)(a) GDPR applies. You may object to the invitation at any time. The data is reviewed at least annually and deleted when no longer required for the survey and lawful customer care.

Trade-fair contacts and lead management

If you provide your data to us at a trade fair or through a business contact, we process in particular your name, company, professional contact details, function, country and the circumstances of the contact to pursue a potential business interest (Art. 6(1)(f) GDPR). We use the data for electronic promotional messages only with consent or where a statutory exception applies. Raw data from trade-fair lead tools is generally deleted within 90 days after the fair ends or the data is transferred. Other lead data is reviewed according to the documented contact status and deleted no later than the end of the defined retention period.

Facebook, LinkedIn Plugin

Our website contains image links to Facebook/Meta and LinkedIn. No connection is established through such a link until you click it. After clicking, you leave our website; Meta Platforms Ireland Limited or LinkedIn Ireland Unlimited Company is primarily responsible for the subsequent processing under its own privacy policy. Processing may include transfers to third countries. Further information: <https://www.facebook.com/privacy/policy> and <https://www.linkedin.com/legal/privacy-policy>.

Youtube Videos

We currently host videos directly on our website and do not use embedded YouTube videos. Where we provide image or text links to YouTube, no connection to YouTube is established until you click the link. If embedded YouTube content is used in the future, it will be integrated in privacy-enhanced mode and loaded only after your consent. Google Ireland Limited is responsible for the subsequent processing by YouTube. Further information: <https://policies.google.com/privacy>.

Google Analytics

We use Google Analytics 4 (GA4), provided by Google Ireland Limited, to measure audience use and improve our website. GA4 is activated only after your consent (Art. 6(1)(a) GDPR; section 25(1) TDDDG additionally applies to storing or reading cookie IDs). Data processed includes pages visited, duration, browser and device category (laptop, tablet or smartphone), cookie IDs and other online identifiers, and approximate location (country, region and city). The IP address is used for transmission and derivation of

approximate location; Google states that IP addresses of EEA users are not logged or stored. The configured retention period for user-level and event-level data is 14 months and is not reset by new activity; aggregated reports may remain available for longer. Google Signals and advertising features are disabled, and GA4 is not linked to Google Ads or our CRM. You may withdraw consent at any time through the cookie settings. Further information: <https://policies.google.com/privacy> and <https://support.google.com/analytics/answer/12017362>.

Google Tag Manager

We use Google Tag Manager, provided by Google Ireland Limited, to manage and control website tags. Tag Manager does not itself create independent user profiles, but services deployed through it may process personal data. The legal basis, data categories and consent requirements depend on the relevant service deployed through Tag Manager. In particular, GA4 is activated only after consent as described above. Further information: <https://developers.google.com/tag-platform/tag-manager> and <https://policies.google.com/privacy>.

10 Additional Information

Links to Third Party websites

Links to third party websites are provided solely as a convenience to you. If you use these links, you will leave the AP Sensing site. AP Sensing has not reviewed all these third-party sites, does not control and is not responsible for any of these sites, their content or their privacy policies. Thus, we do not endorse or make any representations about them, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any of the third-party sites linked to this site, you do so entirely at your own risk.

Changes to the Privacy Statement

All material changes to our Privacy Policy and practices will be posted on this page. The revision date shown at the top of the page will be updated accordingly. As the information at this page can be updated at any time it is recommended to visit this page regularly.

Contact information

Please email questions or comments about our privacy policy to privacy@apsensing.com.