



Privacy and Data Protection Policy

Published date: 7 August 2026

Effective date: 7 August 2026

Version: 1.4

This Privacy and Data Protection Policy outlines how baseworks.tech ("we," "us," or "our") collects, processes, and protects your personal data in accordance with the [General Data Protection Regulation \(GDPR\) EU](#).

Table of contents:

Section 1: Identity and Contact Details of the Data Controller	1
Section 2: Contact Details for Data Protection	1
Section 3: What Personal Data We Collect	2
Section 4: Purposes and Legal Basis for Processing Your Data	2
Section 5: Data Minimization and Accuracy	2
Section 6: Disclosure and Recipients of Your Personal Data	3
Section 7: International Data Transfers	3
Section 8: Data Retention	3
Section 9: Your Rights as a Data Subject	4
Section 10: Right to Withdraw Consent	4
Section 11: Right to Lodge a Complaint	4
Section 12: Security of Your Personal Data	5
Section 13: Changes to This Privacy Policy	5

Section 1: Identity and Contact Details of the Data Controller

The data controller (henceforth also referred to as the “company”) responsible for the processing of your personal data is:

baseworks.tech registered in the Netherlands under Chamber of Commerce number (KvK nummer) 98170643, VAT number (btw-id) NL005312934B1, postal address: Box E1586, Oder 20, 2491DC Den Haag, Netherlands.



If you have any questions, requests or complaints about this policy or our data practices, please contact us at:

privacy@baseworks.tech

Section 2: Contact Details for Data Protection

For any data protection inquiries which fall under the GDPR (EU), please contact our Privacy Team at the contact details provided in Section 1 of this policy.

Section 3: What Personal Data We Collect

We collect and process the following categories of **Personal data you share with us**:

- **Contact Details:** name, delivery address, measurement-site address (only in scope of the Risk Assessment product), invoice address, email address, phone number.
- **Beliefs and Preferences Data:** Data related to declared preferences and routines concerning personal beliefs (except **Special personal data**, as laid out below), along with your declared opinions about them.
- **Interaction Data:** Data concerning interactions and routines in relation to the surrounding spaces and environments with which you interact.
- **Professional Background:** Data concerning the main professional field in which you work (for example: engineering, sales, marketing etc.).
- **Usage and Telemetry Data:** Data concerning your usage, diagnostic information, device malfunction, operational performance, and system interaction with the hardware and software ecosystem.

Special personal data: We do **not** knowingly collect or process special categories of personal data (e.g., data revealing racial or ethnic origin, political opinions, religious beliefs, health data) unless we have a clear legal basis to do so, such as your explicit consent.

In addition to data you share with us directly, we automatically collect certain **Online identifiers belonging to you** when you access our services. This includes:

- Your Internet Protocol (IP) address.

Section 4: Purposes and Legal Basis for Processing Your Data

We will only process your personal data when we have a valid legal basis to do so under the GDPR, which requires but is not limited to your **Consent** and our **Legitimate Interest**. We have your **Consent** where you've agreed to us collecting your personal data, for example when you have ticked a box to indicate that you are happy for us to use your personal data in a certain way or you have signed a consent form. We have a Legitimate Interest when we desire to protect our business from informational attacks such as (but not limited to) spam, denial of service attacks or robotic traffic filtering.



The purposes for which we process your data and the corresponding legal basis are as follows:

Purpose of Processing	Categories of Personal Data	Legal Basis for Processing
Research into business strategies about human-to-environment interaction to determine the feasibility of creating and marketing certain products.	Personal Data you share with us listed in Section 3	Your Consent
Fulfilling your order implies us sharing your contact details with the delivery third-party and payment service you choose during the checkout process.	Contact Details data you share with us listed in Section 3 .	Your Consent
Your IP address is processed to ensure the security, stability, and operational functionality of our service by detecting and mitigating malicious activity, such as DDoS attacks, unauthorized scraping, and other cyber threats.	Online identifiers belonging to you listed in Section 3	Our Legitimate Interest
Assessing the performance, safety, and functionality of hardware and software, including but not limited to the Risk Assessment product..	Usage and Telemetry Data collected during the Risk Assessment monitoring period or the one you explicitly agree to share with us listed in Section 3.	Your Consent

Your personal data is processed solely for the purpose of research used to improve our products and to effectively provide our services to you, and we rely on your explicit consent for this processing. You have the right to withdraw this consent at any time.

Section 5: Data Minimization and Accuracy

We adhere to the principle of data minimization, meaning we only collect and process personal data that is strictly necessary for the purposes outlined in this policy. We take all reasonable steps to ensure the personal data we hold is accurate and up-to-date.

Section 6: Disclosure and Recipients of Your Personal Data



We do not share your personal data with any third parties except in the limited circumstances described below. All personal data is stored in private local and cloud environments that are only accessible to our company. The cloud data is stored by Google LLC (henceforth “Google”) and Amazon Web Services EMEA SARL (henceforth “AWS”) on our behalf, but neither Google nor AWS have access to or process your personal data for their own business interests.

For legal reasons, we may be required to share your personal data with other organizations and authorities. This may include:

- Law enforcement agencies, financial institutions, government bodies, and fraud prevention services to verify your identity, investigate or protect against suspected fraud, and to comply with legal and regulatory obligations, including the ones laid out by the GDPR (EU).
- Other third parties where necessary to:
 - Fulfill any legal or regulatory requirement.
 - Enforce our rights and the rights of our customers or others.
 - In connection with legal claims.
 - In the event of an investigation into suspected or actual criminal or fraudulent activity.
 - If we sell our business or change its legal structure.

Section 7: International Data Transfers

As we provide an international service, we may need to transfer your personal data outside the European Economic Area (EEA) to provide our services. We may send your personal data outside of the EEA to:

- Fulfill global legal and regulatory requirements.
- Provide ongoing support services.
- Share with fraud prevention agencies, regulators, or law enforcement authorities.
- Enable us to provide you with the products or services you have requested.

If we transfer your personal data to another country that does not offer a standard of data protection equivalent to the EEA, we will ensure that your personal data is sufficiently protected. For example, we will make sure that a contract with strict data protection safeguards is in place before we transfer your personal data. In some cases, you may be entitled to ask us for a copy of this contract. In any case, your data will not be used for any other purpose than the one which it was initially collected for.

If you would like more information, please contact us by sending an email to the address referenced in Section 1 of this policy.

Section 8: Data Retention

We will keep your personal data for as long as necessary to fulfill the purpose for which it was collected. The specific time period depends on:

- The length of time required to fulfill the original purpose.
- Our need to comply with relevant legal and regulatory obligations.

Section 9: Your Rights as a Data Subject

Under the GDPR, you have the following rights regarding your personal data, insofar as your personal data is directly or indirectly associated with your identity (i.e. not irreversibly anonymized):

- **The right to be informed:** You have the right to be informed about the collection and use of your personal data.
- **The right of access:** You have the right to request a copy of the personal data we hold about you.
- **The right to rectification:** You have the right to have any inaccurate or incomplete data we hold about you corrected.
- **The right to erasure ("right to be forgotten"):** You have the right to request the deletion of your personal data.
- **The right to restrict processing:** You have the right to request that we restrict the processing of your personal data.
- **The right to data portability:** You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to have it transmitted to another controller.
- **The right to object:** You have the right to object to the processing of your personal data in certain circumstances, including for direct marketing purposes.
- **Rights in relation to automated decision-making and profiling:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

To exercise any of these rights, please contact us at the email address referenced in Section 1 of this policy.

For security reasons, we can't deal with your request if we are not sure of your identity, so we may ask you for proof of your ID. If a third party exercises one of these rights on your behalf, we may need to ask for proof that a third party has been validly authorised to act on your behalf. When you exercise one of these rights, it may take us up to one calendar month to implement your changes. We will usually not charge you a fee when you exercise your rights. However, we are allowed by law to charge a reasonable fee or refuse to act on your request if it is manifestly unfounded or excessive.

Section 10: Right to Withdraw Consent

Since our legal basis for processing your personal data is **Consent**, you have the right to withdraw that consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. To withdraw your consent, please contact us at the email address referenced in Section 1 of this policy.

Section 11: Right to Lodge a Complaint

If you're unhappy with how we've handled your request you can complain to your local data protection authority. In the Netherlands, this is the Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl/>).

Section 12: Security of Your Personal Data



We are committed to ensuring that your personal data is secure. We have implemented appropriate technical and organizational measures to protect your data from unauthorized access, use, alteration, or disclosure. These measures include data encryption and access controls.

Your personal data is kept safe by us by exclusively using encrypted (at rest and in-transit) data management solutions offered by local encrypted devices, Google ([safety statement](#), [data processing addendum](#)) and AWS ([safety statement](#), [data processing addendum](#)). Data access is only possible by [2-step](#) authentication in Google and [MFA](#) authentication in AWS, which we use for all our Google and AWS accounts.

Section 13: Changes to This Privacy Policy

We may update this policy from time to time. The only policy applicable at any point in time is the one with the most recent past effective date relative to today. The **latest version** will be available on our website <https://baseworks.tech/>. We will notify you of any significant changes by posting a new version of the policy on our website or by contacting you by email.

All personal data newly collected from the date when the policy is updated will be processed according to the **latest version** of this policy. For personal data we already hold, we will only apply the new policy to your existing data if the new processing is compatible with the original purposes for which the data was collected, or if we have obtained your prior consent.

Section 14: Governing Language

This policy, as well as any related documents, may be translated into other languages for convenience. In the event of any discrepancies, inconsistencies, or conflicts of interpretation between the English version and the Romanian version (or any other translation), the English version shall prevail and be considered the binding legal text.