BERRYPATH

Privacy Statement for BerryPath

Last updated: 6 July 2026

This privacy statement explains how Sidworks, trading under the name BerryPath, processes personal data when you use BerryPath, the website and the Flow widget. We are established in the Netherlands and process personal data under the General Data Protection Regulation (GDPR).

1. Who we are

Sidworks, trading under the name BerryPath, is responsible for processing account, contact, billing, security and website data.

Detail	Value
Company	Sidworks
Product name	BerryPath
Contact	Contact form on https://www.berrypath.eu/contact
Website	www.sidworks.nl
Chamber of Commerce	94566429
VAT	NL005093105B60

We have not appointed a Data Protection Officer. Privacy questions can be sent to the contact address above.

For data of visitors who use an advice flow on a customer website, the customer is usually the controller. Sidworks processes that data as processor under the processing terms included in the terms.

2. Data we process

We may process the following data:

- Account data, such as name, e-mail address, company, role, language and login status.
- Team and access data, such as invites, permissions, 2FA settings and security logs.
- Subscription and billing data, such as plan, payment status, invoices, VAT data and invoice contacts.
- Support and contact data, such as messages, e-mail address, name and follow-up.
- Product and flow data entered or uploaded by customers, such as product feeds, flow questions, answers, translations, styling and media.
- Advice flow usage, such as answers, result views, product clicks, session ID, locale, source page, device information and technical events.

- Technical data, such as IP address, user-agent, request logs, error logs, rate-limit data and security signals.
- Website data, such as contact form data, functional cookies, language preference, cookie consent choice, reCAPTCHA signals, analytics events and website interaction data after consent.

Customers must not place special category data, payment card data, medical data or other sensitive data in flows, product feeds or support messages unless they have a valid legal basis and appropriate arrangements in place.

3. Why we use data

We use personal data to:

- Create and secure accounts, based on contract and our legitimate interest in secure access.
- Provide the SaaS service, advice flows, product feeds, publications and Flow widgets, based on contract or the customer's processing instructions.
- Manage teams, support, notifications and service messages, based on contract and legitimate interest.
- Handle billing, payment, subscriptions and administrative obligations, based on contract and legal obligations.
- Protect security, prevent misuse, analyse errors, keep logs and maintain availability, based on legitimate interest and legal obligations.
- Improve the product, analytics and flow performance insight, based on legitimate interest or the customer's processing instructions.
- Respond to visitors who contact us through the website, based on legitimate interest or steps before entering into a contract.
- Send optional communication only where permitted by law or consent.

4. Legal bases

We process data on the basis of:

- Performance of a contract, for accounts, subscriptions, support and delivery of the service.
- Legal obligation, for administration and tax data.
- Legitimate interest, for security, logging, fraud prevention, product improvement and business communication.
- Consent, where required, for certain optional features or communication.
- Processing instructions, when we process customer data on behalf of a customer.

Our legitimate interests are keeping the service secure and reliable, preventing abuse, improving the product, supporting customers and protecting our legal and business position. We do not use these interests for unexpected marketing tracking on the public website.

5. Cookies and similar technologies

We use functional and security-focused cookies or browser storage. Examples include sessions, CSRF protection, language settings, registration drafts, 2FA flows and public flow sessions. These are needed for the website and service to work securely.

On the public website, the Google tag uses Google Consent Mode. Before you accept analytics cookies, analytics storage is denied and analytics scripts for Google Analytics and Microsoft Clarity are not loaded. If you decline, analytics cookies stay disabled. If you accept, analytics cookies are enabled for Google Analytics and Microsoft Clarity. Your choice is stored in browser storage so we do not have to ask again on every page. You can reset this choice by clearing browser storage for the website.

When analytics cookies are accepted, Google may process technical information such as page URL, browser and device information, approximate location, IP address and interaction events. Microsoft Clarity may process page views, clicks, scrolling behavior, technical page behavior, browser and device information, approximate location, IP address, heatmaps and session recordings with privacy-sensitive fields masked where possible. We use this to understand how the website is used and to improve the website. We do not use website analytics for advertising or retargeting.

To protect against misuse, Google reCAPTCHA v3 may be used. Technical signals can be sent to Google to assess whether a request is likely legitimate.

The Flow widget may use local storage or session data to keep a flow running smoothly, retain progress, measure analytics and show recommendations. The customer embedding the Flow widget is responsible for informing visitors and obtaining consent where required.

When a workspace owner enables external tracking for a Flow widget, interaction events can be sent to the analytics setup already installed on that website. The customer is responsible for the legal basis, consent where required and the information shown to visitors.

After analytics consent, we also measure clicks to demos and registration, requests to open a demo, and confirmation that a website contact message was sent. These events do not include the contact message, name, email address or form field values. A click to registration is not recorded as a completed account registration.

6. AI, payments and service providers

We may use specialised providers for parts of the service, such as:

- Hosting, infrastructure and storage providers.
- E-mail and transactional delivery providers.
- Payment and invoicing providers.
- Website analytics providers, such as Google Analytics and Microsoft Clarity.
- Logging, monitoring, security and anti-abuse providers.
- AI providers for translation or draft text when AI features are used.
- Support, administration and business tooling providers.

When AI features are used, flow texts or product fields may be sent to an AI provider to create translations or draft text.

We share only the data needed for the relevant service. We enter into appropriate agreements with processors. Payments are handled through a payment provider; we do not store full payment card details.

7. Transfers outside the EEA

Some providers may process data outside the European Economic Area. If this happens, we use appropriate safeguards, such as standard contractual clauses, additional security measures or a valid adequacy decision.

8. Retention

We do not keep data longer than necessary:

- Account and subscription data is kept while the account is active and afterwards as needed for administration, support or legal obligations.
- Invoice and administration data is usually kept for 7 years because of tax rules.
- Security logs, technical logs and error logs are kept as briefly as practical for security and error analysis, normally no longer than necessary for operations, unless longer retention is needed for investigation, abuse prevention or legal defence.
- Import logs and detail logs may be kept briefly and cleaned up automatically.
- Support and contact messages are kept as long as needed for follow-up and the customer relationship.
- Customer data in flows, product feeds and media remains available while the customer uses the service or until the customer deletes it, subject to backups and legal duties.
- Backups are kept temporarily and overwritten on a rolling basis, unless a longer period is needed for security, continuity or legal reasons.

9. Security

We take technical and organisational measures to protect data. Examples include access control, tenant isolation, encrypted connections, logging, 2FA, least privilege, backups, rate limiting and security headers. No online service can guarantee complete security, but we actively reduce risks.

10. Your rights

You can ask us for access, correction, deletion, restriction, portability or objection. If processing is based on consent, you can withdraw that consent.

Send your request through the contact form on https://www.berrypath.eu/contact. We may ask for additional information to verify your identity. We usually respond within one month.

If your request concerns data collected by a customer through an advice flow, we may forward your request to that customer or ask you to contact that customer directly.

11. Complaint

You can always contact us with privacy questions. You also have the right to lodge a complaint with the Dutch Data Protection Authority via autoriteitpersoonsgegevens.nl.

12. Changes

We may update this privacy statement when the service, law or our way of working changes. The latest version is always available on the website and in the application.