Data Processing Agreement

Annex to the Terms of Service. Applies to every subscription, including the free trial. Last updated: 7 November 2026.

1. Parties and roles

This agreement is concluded between the organisation that holds an Ashio account (the “Customer”), acting as controller, and COWBOYS AND WITCHES OÜ (the “Processor”, and “Ashio” throughout these Terms), acting as processor.

Together with section 8 of the Terms of Service, this page is the processing agreement required by Article 28 of the GDPR and Article 9 of the Swiss Federal Act on Data Protection (nFADP). If the two conflict, this page prevails on processing questions.

2. How it is concluded

Article 28(9) GDPR requires the agreement in writing, including in electronic form. Creating an account, or accepting the Terms in the dashboard, accepts this agreement too. No signature is required, and the agreement covers every subscription plan.

If your procurement process requires a signed document, write to legal@ashio.eu and we will send a counter-signed copy of this text.

3. Scope and purpose of processing

Processing is limited to providing the reporting channel described in the Terms: receiving reports, storing them, routing them to the case team the Customer designates, and letting that team follow them up.

- Data subjects: reporters, people named in a report, witnesses, and the Customer’s case handlers.
- Personal data: the content of reports and messages, reporter name or contact details where given, case notes, and account and access data of case handlers.
- Duration: the term of the subscription, plus the retention period the Customer configures.

4. Obligations of the Processor

The Processor shall: (a) process personal data only on documented instructions from the Customer, including as set out in this agreement, and inform the Customer if an instruction appears to infringe the GDPR; (b) ensure that personnel authorised to process the data are bound by confidentiality; (c) implement the technical and organisational measures described in section 7; (d) engage sub-processors only as described in section 5; (e) assist the Customer with data subject requests as described in section 6; (f) assist the Customer with security, breach notification and data protection impact assessments; (g) delete or return the data at the end of the subscription as described in section 8; and (h) make available the information needed to demonstrate compliance and allow for audits as described in section 9.

The Customer is responsible for the lawfulness of the processing, for the instructions it gives, and for the information it provides to reporters and case handlers.

5. Sub-processors

The Customer authorises the sub-processors listed in the sub-processor annex, which forms part of this agreement. That page carries each provider, what it processes, where it runs, and the history of changes to the list.

The Processor gives at least 30 days' notice of any addition or replacement, by email to the billing contact and by updating that page, and the Customer may object on reasonable data protection grounds within that period. The objection channel and the template for it are on the same page. Sub-processors are bound by obligations no less protective than these.

Dodo Payments is not a sub-processor for report data: payment details are collected by Dodo Payments as an independent controller, and Ashio never receives them.

6. Assistance and international transfers

The Processor will forward any request from a data subject it receives to the Customer without responding to it, and will assist the Customer in answering it. The Processor will notify the Customer without undue delay after becoming aware of a personal data breach affecting the Customer's data.

Customer data is stored on infrastructure in Vienna, Austria, inside the EEA, so there is no transfer to a third country and no additional safeguards are required for the storage itself. Customers onboarded from 8 November 2026 are provisioned there directly. Customers onboarded before that date are migrated on 8 December 2026, once the notice period under section 5 has run, and until then their data remains with Infomaniak SA, the Swiss data centre operator named in the annex, whose storage benefits from an adequacy decision of the European Commission. Every other sub-processor named in the annex runs inside the EEA. If a sub-processor outside the EEA is added later, the transfer is covered by the Standard Contractual Clauses set out in the Terms, and it is announced under section 5 before it starts.

7. Security measures

Report bodies and messages are encrypted in the reporter's browser and the server stores ciphertext only, so the Processor cannot read them. Access to case data is restricted to the case team the Customer invites, with role-based permissions. Hosting is in ISO 27001-certified green data centres in Vienna, Austria, operated by netcup GmbH, inside the EEA. The full description is on the security page.

Because encryption is end to end, the Processor's ability to assist with the content of a report is limited to what the Customer can itself decrypt: bulk export, retention and deletion act on ciphertext and case metadata.

8. Deletion and return

The Customer may export cases as PDF at any time while the subscription is active. Retention periods are configurable per organisation, between one and five years after closure, and the reporter-facing privacy notice states the window that applies. After termination the Processor deletes the Customer's data, including backups within the normal backup cycle, unless a statutory retention obligation requires otherwise.

9. Audit and information

The Processor answers security questionnaires, provides the scope of the ISO 27001 certification of its data centres, and answers reasonable written questions about compliance. Where a Customer needs more, an audit may be agreed in writing, subject to confidentiality and to reasonable notice.

10. Liability and governing law

Liability under this agreement is subject to the limitations in the Terms of Service. This agreement is governed by the same law as the Terms. For Swiss processing, the Federal Data Protection and Information Commissioner (FDPIC) is the competent supervisory authority.

11. Contact

Questions about this agreement, or requests for a counter-signed copy: legal@ashio.eu.