

PANScout Privacy Notice

Version 1.1

Effective date: 30 August 2026

1. Who we are

Noema Ltd is a company registered in Gibraltar under company number 125308. Our registered office is 8/5 Naval Hospital Hill, Gibraltar. We provide PANScout and operate <https://panscout.com>.

For the personal data described in this notice, Noema Ltd is normally the controller. Legal notices, privacy questions and requests to exercise data protection rights may be sent to legal@panscout.com.

2. Scope of this notice

This notice explains how we handle personal data in connection with:

- the PANScout website, trial requests and checkout;
- orders, payment status, licence delivery and licence recovery;
- optional passwordless customer accounts, renewals and invoices;
- software and licence downloads;
- business, support, billing, security, legal and privacy communications; and
- security, abuse prevention and service operation.

This notice does not describe an employer's or customer's handling of personal data scanned with PANScout. Those organisations decide why and how they use PANScout and are responsible for their own processing.

3. The local scanning boundary

PANScout is designed to scan locally. In normal use, source files, extracted content, full card numbers, file paths, findings, review notes, scan history and evidence reports are not uploaded to Noema Ltd or to a hosted PANScout scanning service.

PANScout processes possible full payment card numbers in memory where necessary to perform detection. Persisted findings are masked and remain in the customer's environment. Licence validation and scanning do not require a continuous internet connection.

Do not send source files, full card numbers, scan databases, findings or evidence reports to our email addresses. If support exceptionally needs diagnostic context, share only the minimum information authorised by your organisation. The PANScout diagnostic export is designed not to contain file paths, findings or card numbers.

4. Personal data we handle

Depending on how a person interacts with us, we may handle:

- identity and business details, such as name, organisation, role, email address and billing country;
- trial registration and access details, such as the requested installer, evaluation reason, campaign source, an opaque trial-access token hash and its expiry;
- order and licence details, such as product, edition, installation allowance, order status, licence status, validity dates and renewal status;
- limited payment information received from the payment provider, such as payment status, amount, currency, tax result and provider references; we do not need to receive full payment card details;
- account and authentication details, such as the order email, organisation membership, short-lived sign-in and confirmation records, session records and recovery requests;

- delivery and download records, such as whether a licence email was sent and whether an authenticated licence or software download was requested;
- communications with business, support, billing, security, legal or privacy contacts and the information provided in them;
- security and operational information, such as event time, request outcome, rate-limit or abuse signals, and limited technical request information processed by our hosting provider; and
- invoice, refund, dispute and accounting records.

We use consent-aware Google Analytics 4 and Google Ads conversion measurement on the public website. This measurement is limited to website and acquisition activity, including the page path, event time, browser or device category, approximate location derived by Google from the technical request, consent state and campaign or conversion information. PANScout removes query strings and fragments from measured page addresses. Measurement does not receive PANScout application activity, trial-form contents, email addresses, organisation names, filenames, paths, findings, reports, card numbers, licence keys, authentication tokens or Checkout session references. We do not enable personalised advertising, retargeting or Google signals.

Cloudflare uses the country associated with the incoming request to return only whether PANScout should ask for prior consent. We do not return Cloudflare's country value to the page or send that value as a PANScout analytics event or parameter. For visitors in the EEA, United Kingdom, Switzerland and Gibraltar, for locations not yet approved for automatic measurement, and whenever the location cannot be determined, optional storage is denied until the visitor chooses. Google consent mode may send limited storage-free measurement requests containing information such as the sanitized page address, event time, technical request information and consent state before that choice. For visitors in the United States, analytics and conversion measurement may be enabled without displaying the consent banner, subject to the browser's Global Privacy Control and the visitor's saved choices.

The footer provides a Privacy choices control wherever measurement is configured. A strictly necessary first-party preference cookie records the policy version, chosen categories and time of the choice for up to six months. A visitor can change the choice at any time. After a person requests a trial, a separate strictly necessary first-party cookie remains available for up to 14 days so that the browser can obtain another supported installer without repeating the form. The trial cookie contains only an opaque random token; the corresponding hash and expiry are stored by us.

5. How we obtain personal data

We obtain personal data:

- directly from the person or organisation requesting a trial, placing an order, accessing an account or contacting us;
- from our payment provider when it confirms an order, payment, renewal, refund or dispute;
- from our website, hosting, authentication, email and delivery systems when they perform a requested or security-related operation;
- from consent-aware website analytics and advertising measurement where enabled under this notice; and
- from an organisation that authorises a person to administer its PANScout licences.

6. Why we use personal data and our legal bases

We use personal data only where we have an appropriate legal basis.

Contract and pre-contract steps

We use identity, trial, order, account, payment-status and delivery information to provide requested trial access, process an order, issue and recover a licence, provide optional account access, make invoices available, manage renewal and provide requested support.

Legal obligations

We use and retain information where necessary for accounting, tax, company, fraud prevention, sanctions, dispute, data protection or other legal obligations.

Legitimate interests

We use proportionate information to protect accounts and licence delivery, prevent abuse and fraud, maintain service reliability, investigate security reports, establish or defend legal claims, improve support and understand aggregate website and campaign performance where prior consent is not required. We balance these interests against the rights and expectations of affected individuals and provide persistent privacy choices.

Consent

Where prior consent is required, consent is the basis for optional analytics or advertising storage and the associated measurement. Consent can be refused or withdrawn without affecting the website, trial, purchase or PANScout application. If we offer optional marketing communications, they use the consent or other lawful basis required for the recipient and market. Transactional licence, security, account and billing messages are not marketing messages.

7. Accounts and automated decisions

A minimal passwordless account may be prepared after a verified purchase so the purchaser can access licences, invoices and renewal information. Using the account is optional and is not required to run PANScout.

Account access uses a short-lived link sent to the order email. We do not use permanent device identifiers for licence enforcement. We do not make decisions producing legal or similarly significant effects solely through profiling or automated decision-making.

8. Who receives personal data

We disclose only the information needed for the relevant service. Recipient categories may include:

- Cloudflare, for website hosting, security, storage and related infrastructure;
- Google, for consent-aware website analytics and advertising conversion measurement;
- the payment provider identified at checkout, for payment processing, tax handling, refunds, disputes and fraud prevention;
- the transactional email provider used for account and licence delivery;
- professional advisers, auditors, insurers and service providers subject to appropriate confidentiality and data protection terms;
- public authorities, regulators, courts or law enforcement where disclosure is legally required; and
- a successor to the relevant business where a lawful corporate transaction occurs.

We review our provider arrangements and contractual safeguards when the services we use change materially, and update this notice where appropriate.

We do not sell personal data.

9. International transfers

Some providers may process personal data outside Gibraltar. Where a transfer is restricted under Gibraltar data protection law, we use an applicable adequacy decision or recognised contractual and organisational safeguards. We assess the transfer and apply additional safeguards where appropriate.

Information about the safeguards relevant to a particular transfer may be requested through legal@panscout.com.

10. Retention

We keep personal data only for as long as needed for the purpose described and then delete or anonymise it, unless a legal obligation, security incident, dispute or legal claim requires longer retention.

Our retention schedule is:

- uncompleted authentication challenges and links expire after a short period measured in minutes;

- trial-access cookies and their corresponding server-side token records expire after no more than 14 days;
- website measurement preference cookies expire after no more than six months, or earlier when the visitor clears them;
- Google Analytics event-level data is configured for retention for no more than two months; aggregated reports may remain available for longer without the underlying event-level record;
- authenticated browser sessions expire after no more than 12 hours and sensitive account actions may require a newer sign-in;
- short-lived recovery and abuse-prevention records are retained only as needed to enforce the applicable cooldown or security control;
- order, licence, invoice, refund and accounting records are retained for the active commercial relationship and the period required by applicable accounting, tax and legal-claims rules;
- ordinary support correspondence is normally retained for up to 24 months after the request closes;
- routine security and access audit events are normally retained for up to 12 months; and
- records connected with an incident, dispute, fraud concern or legal obligation may be retained until the matter and any relevant claims period have ended.

We maintain deletion and review procedures designed to apply this schedule.

11. Security

We use technical and organisational measures appropriate to the nature of the personal data and the risks involved. These include restricted administrative access, passwordless recent-authentication controls, encrypted transport, private licence storage, signed licence files, secret separation, provider webhook verification, security logging and data minimisation.

No system can be guaranteed completely secure. Security concerns about PANScout should be reported to security@panscout.com without including customer files or payment card data.

12. Individual rights

Subject to Gibraltar data protection law and any applicable exceptions, individuals may have rights to:

- be informed about processing;
- obtain access to their personal data;
- correct inaccurate or incomplete data;
- request deletion or restriction;
- object to processing based on legitimate interests or to direct marketing;
- withdraw website measurement consent at any time through the Privacy choices control;
- receive qualifying data in a portable format; and
- complain to the Gibraltar Regulatory Authority, acting as Information Commissioner.

Requests may be sent to legal@panscout.com. We may request proportionate information to verify identity and authority before disclosing or changing account information.

The Gibraltar Regulatory Authority provides current data protection information at <https://www.gra.gi/data-protection>.

13. Business contacts and other people

An organisation may provide contact details for an employee, consultant or administrator. The organisation should ensure that it is authorised to do so and that the person receives relevant privacy information. Account administrators must not use account access to obtain another person's information without authority.

14. Changes to this notice

We may update this notice when the product, providers or legal requirements change. The current version and effective date will be published at <https://panscout.com>. Material changes affecting an active account or renewal will be communicated where appropriate.

15. Contact

Legal and privacy: legal@panscout.com

Product support: support@panscout.com

Billing and payments: billing@panscout.com

Security reports: security@panscout.com

Registered office: 8/5 Naval Hospital Hill, Gibraltar