

PRIVACY POLICY

NOMOS Intelligence

Last updated: 11 August 2026

ABOUT THIS PRIVACY POLICY

This Privacy Policy describes how NOMOS Intelligence, currently operating as a pre-incorporation project in Belgium ("NOMOS", "we", "us", or "our"), may collect, use, store, disclose, and otherwise process personal data when you use our services ("Services").

Before publication, the current data controller must be identified here: [INSERT FULL NAME(S) OF CURRENT DATA CONTROLLER(S)]. Following incorporation, this section will be updated to identify NOMOS Intelligence SNC, its registered office, enterprise number, and other legally required company details.

For privacy questions or requests, contact us at privacy@nomos-intel.eu.

This Policy applies when you:

- visit <https://nomos-intel.eu> or another NOMOS website that links to this Policy;
- use the NOMOS Intelligence pilot;
- request or receive access to a NOMOS client account;
- submit research requests, files, or other material through the Services;
- communicate with us about our Services, prospective engagements, marketing, or events.

NOMOS is developing a manually managed open-source intelligence pilot for institutional, corporate, NGO, and media clients. Approved clients can submit research requests and relevant files, monitor project progress, and securely receive completed reports. The pilot is not currently an automated marketplace.

SUMMARY OF KEY POINTS

We process personal data only where we have a valid legal basis and only for purposes connected with operating, securing, administering, and improving the Services, managing approved client relationships and research assignments, communicating with users, and complying with applicable law.

We may process names, professional contact information, organisation or employer, account and authentication information, research-request details, uploaded files, communications with NOMOS, technical logs, and limited publicly available online information relevant to approved FIMI research.

We do not intentionally request special-category personal data from clients or users. Such information may exceptionally appear incidentally in publicly available material relevant to an approved research assignment. Where this occurs, we will minimise the processing and handle it in accordance with applicable law.

Research requests and uploaded client files are not publicly posted. Access is limited to authorised NOMOS personnel and, where necessary, assigned analysts and senior reviewers who require the information for the relevant assignment.

At the time of publication, NOMOS uses only strictly necessary cookies for authentication, secure sessions, and core portal functionality. If this changes, this Policy and any applicable Cookie Policy or consent mechanism will be updated before non-essential tracking technologies are enabled.

You may exercise applicable data-protection rights by contacting privacy@nomos-intel.eu or using <https://nomos-intel.eu/privacy-request>.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?
2. HOW DO WE USE YOUR PERSONAL DATA?
3. WHAT LEGAL BASES DO WE RELY ON?
4. WHEN AND WITH WHOM DO WE SHARE PERSONAL DATA?
5. COOKIES AND SIMILAR TECHNOLOGIES
6. INTERNATIONAL DATA TRANSFERS
7. HOW LONG DO WE KEEP PERSONAL DATA?
8. HOW DO WE KEEP PERSONAL DATA SAFE?
9. MINORS
10. YOUR PRIVACY RIGHTS
11. NOMOS PILOT AND RESEARCH SCOPE
12. PUBLICLY AVAILABLE RESEARCH INFORMATION
13. SUBMISSION RESTRICTIONS
14. PRIVATE ACCESS TO REQUESTS AND FILES
15. CHANGES TO THIS POLICY
16. CONTACT AND DATA-PROTECTION REQUESTS

1. WHAT INFORMATION DO WE COLLECT?

Personal data you provide to us

We collect personal data that you voluntarily provide when you request access, register for or use the Services, submit a research request or file, communicate with us, or otherwise interact with NOMOS.

Depending on your interaction with us, this may include:

- names;
- email addresses and other professional contact details;
- job titles;
- organisation or employer;
- passwords, authentication data, and account identifiers;
- research-request details;
- files and documents uploaded by users;
- communications with NOMOS; and
- other information you choose to provide in connection with an approved request or engagement.

Publicly available research information

For approved FIMI research assignments, NOMOS may process limited publicly available online identifiers and content relevant to the research purpose, such as social-media usernames, public profile information, posts, and interactions. Further safeguards are described in Sections 11 and 12.

Special-category personal data

NOMOS does not intentionally request clients or users to submit special-category personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data used for identification, health data, or data concerning a person's sex life or sexual orientation.

Such information may exceptionally appear incidentally in publicly available source material relevant to an approved research assignment. Where processing is necessary and lawful, NOMOS will limit it to what is reasonably necessary for the approved purpose and apply appropriate safeguards. Clients must comply with the submission restrictions in Section 13.

Information collected automatically

When you visit or use the Services, our systems may automatically receive technical and usage information needed to operate and secure the Services. This may include IP address, browser and device characteristics, operating system, language preferences, referring URLs, approximate country or region, timestamps, pages or features accessed, and diagnostic or security logs.

This information is primarily used to maintain security, authenticate sessions, troubleshoot errors, and understand the technical operation of the Services. We do not currently use behavioural advertising or advertising trackers.

Information from other sources

We may receive limited professional or organisational information from public sources or from people or organisations that communicate with us, for example to verify an applicant's professional or institutional affiliation, manage a prospective client relationship, or carry out an approved research assignment.

We do not currently purchase marketing profiles, intent data, or advertising audiences from data brokers for behavioural advertising.

2. HOW DO WE USE YOUR PERSONAL DATA?

We use personal data for the following purposes:

- Account creation and authentication: to create, authenticate, administer, and secure approved user accounts.
- Service delivery: to receive, scope, manage, and perform approved research requests and to securely deliver associated reports and files.
- Access and institutional verification: to assess access requests and verify professional or institutional affiliation where appropriate.
- Client relationship administration: to communicate with representatives of prospective and existing client organisations and administer the relationship.
- Support and communications: to answer enquiries, provide support, and send administrative information about the Services, policies, or relevant changes.
- Security and fraud prevention: to protect accounts, systems, users, and the Services; investigate suspected misuse; and maintain security logs.
- Legal compliance and legal claims: to comply with applicable legal obligations and to establish, exercise, or defend legal claims.

- Vital interests: in exceptional circumstances, to protect a person's life or physical safety where processing is necessary.

Retention periods by purpose

Unless a longer period is required or permitted by law or a separate agreement:

- Account data: for the duration of the active account and generally for 6 months after account deactivation; expired authentication tokens are retained only as technically necessary.
- Project and service-delivery data: for the duration of the engagement and generally for 6 months after project completion, unless the client agreement requires earlier deletion or longer retention is needed for legal obligations or claims.
- Support and enquiry records: generally for 12 months after the last substantive communication; unsuccessful access requests may be deleted earlier when no longer needed.
- Administrative client-relationship records: for the duration of the relationship and generally for 12 months after it ends, unless longer retention is required for legal or accounting purposes or legal claims.
- Security and technical logs: generally for 90 days. Records linked to a suspected security incident may be retained for up to 12 months or longer where reasonably necessary to investigate or address the incident.

3. WHAT LEGAL BASES DO WE RELY ON?

Where the GDPR applies, we process personal data only where a valid legal basis is available.

Depending on the circumstances, this may include:

- Performance of a contract or steps before entering into a contract, where processing is necessary to provide requested Services or manage an engagement.
- Legitimate interests, where processing is reasonably necessary for our legitimate business or security interests and those interests are not overridden by the rights and freedoms of the individual. These interests may include restricting the pilot to appropriate authorised organisations, protecting the Services, administering professional relationships, preventing misuse, and establishing or defending legal claims.
- Consent, where we specifically ask for consent for a particular processing activity. Consent may be withdrawn at any time without affecting processing already carried out lawfully.
- Legal obligations, where processing is necessary to comply with applicable law, regulatory requirements, or lawful orders.
- Vital interests, in exceptional circumstances where processing is necessary to protect someone's life or physical safety.

Where special-category personal data is processed, NOMOS will rely on an applicable condition under data-protection law in addition to an Article 6 legal basis, where required.

4. WHEN AND WITH WHOM DO WE SHARE PERSONAL DATA?

We disclose personal data only where reasonably necessary for the purposes described in this Policy or where required by law.

Recipients may include:

- cloud, hosting, infrastructure, authentication, or security service providers;
- communication and collaboration service providers;
- authorised analysts and senior reviewers assigned to the relevant research project;
- legal, accounting, compliance, and other professional advisers;

- public authorities, regulators, courts, or law-enforcement bodies where disclosure is legally required or otherwise lawful; and
- a purchaser, successor, investor, or relevant adviser in connection with a genuine financing, restructuring, merger, acquisition, or transfer of the business, subject to appropriate confidentiality and data-protection safeguards.

Where a third party acts as our processor, we will use appropriate contractual and organisational safeguards as required by applicable data-protection law.

5. COOKIES AND SIMILAR TECHNOLOGIES

At the time of publication, NOMOS uses only cookies and similar technologies that are strictly necessary to provide requested functionality, authenticate users, maintain secure sessions, protect the portal, and support essential technical operation.

These technologies are not used for behavioural advertising or advertising profiling. Where required, we provide information about the purpose and duration of strictly necessary cookies.

If NOMOS later introduces analytics, advertising, or other non-essential cookies or tracking technologies, we will update our disclosures and implement any consent mechanism required by applicable law before enabling them.

6. INTERNATIONAL DATA TRANSFERS

We do not state in this Policy that NOMOS data is hosted in any particular country unless that location has been verified with the relevant service provider.

Some service providers we use may process personal data outside the country in which the user is located. Before relying on such a provider for a transfer of personal data outside the European Economic Area, we will assess the applicable transfer mechanism and use safeguards required by data-protection law.

Where applicable, such safeguards may include a European Commission adequacy decision, the European Commission's Standard Contractual Clauses, or another lawful transfer mechanism. Information about applicable safeguards will be made available where required by law.

This section will be updated if and when NOMOS confirms the locations of its material hosting and processing providers.

7. HOW LONG DO WE KEEP PERSONAL DATA?

We retain personal data only for as long as reasonably necessary for the purposes described in this Policy, unless a longer period is required or permitted by law, a client agreement, or the need to establish, exercise, or defend legal claims.

When personal data is no longer required, we will delete or anonymise it where reasonably practicable. Where immediate deletion is not technically possible, for example because data remains temporarily in secure backups, access will be restricted until deletion or overwriting occurs in accordance with the relevant retention cycle.

8. HOW DO WE KEEP PERSONAL DATA SAFE?

We use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

Measures may include access controls, authentication, restricted project access, secure communications, logging, and other safeguards appropriate to the nature of the Services and the information processed.

No internet transmission or storage system can be guaranteed to be completely secure. If we become aware of a personal-data breach, we will assess and respond to it in accordance with applicable data-protection law.

9. MINORS

The Services are intended for professional and organisational use and are not intended for persons under 18 years of age. Persons under 18 may not create an account or submit a research request through the Services.

If we learn that we have collected personal data directly from a person under 18 in circumstances not permitted by law, we will take reasonable steps to delete or otherwise appropriately address the data.

10. YOUR PRIVACY RIGHTS

Depending on applicable law and the circumstances, you may have rights including:

- the right to access personal data concerning you and obtain a copy;
- the right to correct inaccurate or incomplete personal data;
- the right to request erasure in applicable circumstances;
- the right to restrict processing in applicable circumstances;
- the right to object to processing based on legitimate interests in applicable circumstances;
- the right to data portability where applicable;
- the right to withdraw consent at any time where processing is based on consent; and
- rights relating to certain automated decision-making, where applicable.

To exercise your rights, contact privacy@nomos-intel.eu or use <https://nomos-intel.eu/privacy-request>. We may request information reasonably necessary to verify your identity and protect personal data from unauthorised disclosure.

We will respond within the time limits required by applicable law. If you believe your data-protection rights have been infringed, you also have the right to lodge a complaint with the competent supervisory authority. For processing for which the controller is established in Belgium, this may include the Belgian Data Protection Authority.

11. NOMOS PILOT AND RESEARCH SCOPE

NOMOS operates a manually managed open-source intelligence pilot focused on FIMI campaigns, public narratives, coordinated networks, and observable organisational behaviour. The pilot is not currently an automated intelligence marketplace.

NOMOS does not offer private-person investigations, background checks, or investigations concerning personal disputes through the pilot.

12. PUBLICLY AVAILABLE RESEARCH INFORMATION

For approved research assignments, NOMOS may process publicly available online identifiers and content relevant to FIMI analysis, including social-media usernames, public profile information, posts, and interactions.

Personal identifiers will be processed only where reasonably necessary for the approved research purpose and will be minimised, aggregated, or pseudonymised where identification is unnecessary.

Public availability does not by itself remove information from the scope of data-protection law. NOMOS will assess the necessity, relevance, and proportionality of processing in light of the approved research purpose.

13. SUBMISSION RESTRICTIONS

Clients and users must not submit information that is unnecessary for the approved research purpose. In particular, they must not knowingly submit:

- account passwords, authentication credentials, or access tokens;
- confidential-source identities unless specifically authorised and covered by an appropriate written agreement;
- special-category personal data unless NOMOS has expressly agreed in writing that the processing is necessary, lawful, and subject to appropriate safeguards;
- unlawfully obtained material; or
- personal data unrelated to the approved research purpose.

NOMOS may reject a request, restrict access to submitted material, or require removal and resubmission where information falls outside the permitted scope of the pilot.

14. PRIVATE ACCESS TO REQUESTS AND FILES

Research requests and uploaded files are not publicly posted. They are accessible only to authorised NOMOS personnel and, where necessary, assigned analysts and senior reviewers who require the information to perform or review the relevant assignment.

Access is limited according to the client organisation, project assignment, and role. Where an analyst or reviewer does not need particular information to perform the assignment, access should not be granted.

15. CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time to reflect changes in our Services, processing activities, providers, or legal obligations. The revised version will show an updated date at the top.

Where a change materially affects how we process personal data, we will provide additional notice where required by applicable law.

16. CONTACT AND DATA-PROTECTION REQUESTS

For privacy questions, complaints, or requests to access, correct, delete, restrict, or otherwise exercise rights concerning personal data, contact:

NOMOS Intelligence (pre-incorporation project)

Current data controller(s): [INSERT FULL NAME(S) BEFORE PUBLICATION]

Email: privacy@nomos-intel.eu

Privacy request form: <https://nomos-intel.eu/privacy-request>

Postal/contact address: [INSERT A VALID CONTACT ADDRESS BEFORE PUBLICATION]

After incorporation, this section will be updated to identify NOMOS Intelligence SNC, its registered office, enterprise number, and other required details.

PRE-PUBLICATION NOTE - REMOVE BEFORE WEBSITE LAUNCH: Do not publish the Policy until the current data controller name(s) and a valid contact address have been inserted. Confirm the actual cookies used by the live website. No server or hosting country is asserted in this draft because NOMOS has not yet verified that information. After incorporation, replace the pre-incorporation controller details with the exact registered company details.