



RFP & TENDER INFORMATION

EuroChat

Secure, sovereign communication for European government.

A federated and fully European communication platform that supports classification in line with applicable laws, regulations and relevant security frameworks. The platform provides facilities for secure communication, information management and archiving, fitting the requirements placed on government organisations. Built for governments that adopt digital sovereignty, security by design and privacy by design as guiding principles. This pack bundles functional, legal, security, archiving and sovereignty characteristics, providing a solid basis for procurement, tender and market-exploration processes.

PUBLISHER

Wroote, wroote.eu

DOCUMENT VERSION

1.0

STATUS

Informational, not a binding offer (sec. 11)

PRODUCT

EuroChat, government communication platform

AS OF

23 June 2026

CONTACT

pilot@wroote.eu · privacy@wroote.eu

12

classification levels

8

interface languages

100%

EU hosting, no hyperscaler

0

undisclosed limitations

About this document

This information pack supports procurement, IT and information-security officers in evaluating and including EuroChat in a tender or market-exploration process (e.g. statement of requirements, market consultation, RFI/RFP). It brings together the functional, legal, security and sovereignty characteristics of the platform in one place, with explicit reference to the applicable legal framework.

Honesty first (why status labels?). EuroChat is a platform in active development with a working SaaS / pre-production environment (production runs at the customer) and a published roadmap. To prevent an unintentionally broad claim from ending up in a tender document, every capability in this document carries a status label. This reflects Wroote's internal conformity records (architecture decisions and conformity dossier) and is deliberately conservative.

Status label	Meaning
	Demonstrably implemented and in use in Wroote's SaaS / pre-production environment; production runs at the customer.
	Partly implemented; the core works, with stated limitations or an ongoing rollout.
	Designed and/or decided (architecture decision), not yet rolled out. Not to be read as a commitment.

Wroote & EuroChat

Wroote is the organisation behind **EuroChat**, a secure communication platform for European government. EuroChat is not a generic chat app but a platform for *classified* government communication: classification, archiving, audit and federation are core functionalities, not optional.

- **Positioning:** replacing commercial chat platforms (such as WhatsApp, Signal, Teams, Webex) with a federated, European solution that remains under your own control.
- **Target audience:** Dutch and European government organisations; the first phase focuses on the Dutch central government (Rijksoverheid).
- **Ambition:** growth into a European, federated platform across multiple member states.

Functional overview

Capability	Description	Status
Secure messaging	One-to-one and group chat on the open Matrix protocol (Synapse homeserver).	
Classification (12 levels)	Dynamic per-organisation classification catalogue with policy binding (see sec. 3).	

Capability	Description	Status
Video conferencing	Integrated WebRTC conferences via a self-hosted LiveKit SFU (incl. TURN/coturn for NAT traversal); no external service.	AVAILABLE
Archiving & compliance	Archiving, search, legal hold, integrity verification, compliance export (see sec. 5).	AVAILABLE
Audit trail	Tamper-resistant logging via a cryptographic hash chain.	AVAILABLE
Roles & authorisation	Administrator / Archivist / User with zero-trust, database-validated authorisation.	AVAILABLE
Multilingual	8 languages in the user interface (see sec. 6).	AVAILABLE
Identity, SSO & provisioning	Keycloak (OIDC, PKCE); SAML2 brokering for ministry IdP integration; automated identity provisioning to the underlying services.	AVAILABLE
Bridges (WhatsApp/Signal)	Controlled integration with external channels via mautrix bridges, under policy. Note: classification and encryption guarantees do not apply to bridged external channels.	AVAILABLE
Multi-factor authentication (TOTP)	TOTP MFA (TOTP app, e.g. FreeOTP) enforced per tenant; token gate (amr validation) and in-app enrolment wizard.	AVAILABLE
MFA strength per classification level	Hardware/passkey requirements and step-up bound to classification (factor classes, ADR-0028).	ROADMAP
Federation (protocol & partner management)	Matrix federation at the protocol level; registration and configuration of federated partners in the admin UI.	AVAILABLE
Federation trust policy (cross-org)	Federation Trust Policy: validation/mapping of remote factor classes, untrusted-default, cross-org enforcement (ADR-0028, D8).	ROADMAP

3 Classification (as a policy layer)

In EuroChat, classification is a **policy layer**, not merely a label. The catalogue supports a layered set of levels that an organisation can activate/deactivate and bind to policy itself. The catalogue is served dynamically (colours, policy and translations per language) and drives behaviour elsewhere in the platform (federation rules, archiving/retention periods, MFA requirements, encryption enforcement).

Currently in scope for electronic processing (SaaS)

PUBLIC, INTERNAL, DEPARTMENTAL, CONFIDENTIAL (and equivalent levels)

Higher classifications. Secret, state-secret and the NATO- and EU-classified variants are currently not processed electronically via EuroChat (laws and regulations). These are foreseen for an **on-prem / sovereign deployment at the customer with an HSM, after the required accreditation process** (see sec. 9): future, not a commitment.

AVAILABLE Dynamic catalogue API, policy binding and visible classification indicators in the interface, within the in-scope levels.

4 Legal & compliance framework

EuroChat is designed to align with the Dutch and European framework for government information. The overview below links each framework to the way EuroChat supports it, with an honest distinction between what the platform delivers technically and what requires policy, decision-making or formal certification on the part of the customer.

4.1 Privacy: GDPR (Regulation (EU) 2016/679)

- **Role allocation:** the procuring government organisation is typically the *controller*; Wroote acts as *processor*. A data processing agreement (Art. 28 GDPR) is part of the contract phase.
- **Privacy by design & by default (Art. 25):** data minimisation, classification and access restriction are embedded in the design.
- **DPIA support:** architecture, data flows and security measures are documented so that a data protection impact assessment (Art. 35) can be carried out by the customer on a sound basis. **PARTIAL**, documentation available; a formal DPIA is the customer's responsibility.
- **No processing outside the EU:** all data processing and storage take place within the EU (see sec. 7), avoiding transfers to third countries.

4.2 Information security: NIS2 & BIO2 (ISO 27002)

- **NIS2 (Directive (EU) 2022/2555):** EuroChat supports customers subject to NIS2 with measures around access management, logging/monitoring, incident traceability and supply-chain transparency (open source, no hyperscaler dependency).
- **BIO2 (based on ISO 27002; successor to the BIO, the Dutch public-sector security baseline):** the platform is designed according to security by design and aligns with the BIO2 / ISO 27002 themes (access control, logging, cryptography, classification). **ROADMAP**, a formal BIO2 / ISO 27001/27002 audit or certification has not been completed at this time; this is part of the roadmap and open to discussion on request. No certifications that have not been obtained are claimed in this document.

4.3 Archiving & openness: Archiefwet, Woo, DUTO/MDTO

- **Archiefwet (Dutch Public Records Act):** EuroChat provides the technical building blocks for sustainable and reliable information management. Full compliance additionally requires policy and decision-making at the customer (selection list, retention periods, destruction and transfer decisions); technology alone is not sufficient.
- **DUTO/MDTO:** archives carry a metadata profile and are captured in a sustainable format (PDF/A-3), with integrity anchoring. See sec. 5 for the exact conformity status per layer.
- **Woo (Dutch Open Government Act):** searchability, export and recording of disclosure restrictions support freedom-of-information requests; the actual disclosure decisions remain with the customer.

4.4 Procurement: Dutch Procurement Act 2012 / Directive 2014/24/EU

EuroChat is built from open standards and open-source components without vendor lock-in (see sec. 7), aligning with proportionality, interoperability and award on the basis of the most economically advantageous tender (MEAT). The conformity matrix in sec. 9 can serve as a basis for a statement of requirements or a declaration of conformity in a tender.

For **defence and security-sensitive** contracts, the **Dutch Procurement Act for the defence and security domain (ADV)** may apply instead of the Procurement Act 2012; it is increasingly required for critical systems. EuroChat's open-standards and sovereignty profile aligns with it.

4.5 Open standards: Forum Standaardisatie ("comply or explain")

Standard	Use in EuroChat
Matrix	Open, federated messaging protocol, the core of the platform.
OpenID Connect / OAuth 2.0	Authentication and authorisation (Keycloak, PKCE).
SAML 2.0	Identity brokering for integration with existing government IdPs.
TLS	Encryption of external transport.
WebRTC (+ TURN/STUN)	Real-time audio/video; NAT traversal via self-hosted coturn.
S3 (object storage API)	Storage interface, prevents storage lock-in.
PDF/A	Sustainable archival format.

5 Archiving & conformity (detailed)

The archiving flow is deliberately built from **three separate layers**; each layer claims only what it guarantees. **DUTO ≠ Archiefwet ≠ WORM**, no overlapping claims are made.

Layer	Guarantees	Does <u>not</u> guarantee	Status
DUTO/MDTO information quality	Findability, accessibility, sustainable format (PDF/A-3), reliability (metadata, authenticity via hash).	That the Public Records Act has been satisfied.	AVAILABLE
Archiefwet management processes	Service controls for retention/selection; grounds registration.	Full compliance without policy and decision-making at the customer.	PARTIAL
WORM storage immutability	Technical integrity/retention at the storage layer (Object Lock, governance mode).	Compliance-mode WORM; a holder of storage root credentials can technically override retention.	ROADMAP

Already available: archiving, search, download, **legal hold** (with an immutable history), **integrity verification** (SHA-256), **compliance export** and a DUTO metadata profile with PDF/A-3 rendition. An independent timestamp (RFC 3161), the WORM immutability layer and **WARC export** (web archive format) are on the roadmap; these limitations are stated explicitly and deliberately.

6 Multilingual support

AVAILABLE The user interface is fully built with an i18n system (no hard-coded text) and available in **8 languages**: Dutch, English, French, German, Spanish, Italian, Polish and Czech.

7 Digital sovereignty & open source

- **EU hosting:** the entire infrastructure runs within the EU (Hetzner, Germany). All data storage (object storage, database) resides on EU territory. **AVAILABLE**
- **No hyperscaler dependency:** deliberately no use of Microsoft Azure, Amazon AWS or Google Cloud, thereby avoiding exposure to, among others, the U.S. CLOUD Act.
- **No paid vendor lock-in:** use of the free, open-source Synapse homeserver (AGPL), with no Element Server Suite or other paid Matrix products.
- **Open-source foundation:** Synapse (AGPL), LiveKit (Apache 2.0), Keycloak, PostgreSQL, MinIO (S3-compatible). Standard interfaces (Matrix, OIDC, S3) enable migration and exit.

Note (transparency): "EuroChat is open source" is not currently claimed as a product-wide property. The platform builds on open-source components; the possible open-sourcing of the EuroChat application code itself is a separate consideration.



8 Security (security by design)

Measure	Notes	Status
Transport encryption (external)	TLS 1.3 as the standard, TLS 1.2 as fallback, on all external endpoints.	AVAILABLE
Identity & authorisation	Immutable canonical identity; zero-trust, database-validated authorisation; fail-secure (deny when in doubt).	AVAILABLE
Audit trail	Tamper-resistant hash chain over security and archiving events.	AVAILABLE
Multi-factor authentication (TOTP)	TOTP MFA (TOTP app, e.g. FreeOTP) enforced per tenant via Keycloak (amr validation); in-app enrolment wizard and status endpoint.	AVAILABLE
MFA strength per classification level	Factor classes (passkey / hardware token) and step-up bound to classification; phased rollout (ADR-0028).	ROADMAP
End-to-end encryption (E2EE)	Enforced for the highest in-scope classified rooms; lower levels not yet E2EE by default. The recovery mechanism is under review.	PARTIAL
Encryption at rest	Disk/database/object-storage encryption is largely not yet implemented; included in a phased improvement plan.	ROADMAP
Internal service encryption	Traffic between internal services currently runs partly unencrypted within the trusted host; mTLS is on the roadmap.	ROADMAP

Maturity & honesty. EuroChat is in a pilot/build-up phase. The security measures marked **ROADMAP** above (encryption at rest, internal mTLS, the definitive E2EE recovery model) are named, captured in architecture decisions and planned. For processing highly classified data they are considered preconditions. Wroote will share the full security and conformity dossier on request under NDA during a tender/pilot process.

9 Conformity matrix (short)

Usable as a basis for a statement of requirements or a declaration of conformity. Status labels per the reading guide at the top of this document.

Requirement / capability	Status	Notes
Secure messaging (open protocol)	AVAILABLE	Matrix/Synapse.
Classification with policy enforcement	AVAILABLE	Layered catalogue; highest levels not yet electronic (see sec. 3).
Archiving with legal hold & integrity	AVAILABLE	SHA-256 verification, compliance export.
Sustainable archival format (PDF/A, DUTO metadata)	AVAILABLE	Independent timestamp: roadmap.
Tamper-resistant audit trail	AVAILABLE	Hash chain.
SSO via OIDC; SAML2 brokering	AVAILABLE	Keycloak; integration with government IdP possible.
EU data sovereignty (EU hosting, no hyperscaler)	AVAILABLE	Hetzner (DE); open source.
Multilingual UI	AVAILABLE	8 languages.
Self-hosted video conferencing	AVAILABLE	LiveKit (Apache 2.0).
Multi-factor authentication (TOTP, per tenant)	AVAILABLE	amr validation + enrolment wizard.
MFA strength enforced per classification level	ROADMAP	Hardware/passkey + step-up per level (ADR-0028).
Federation, protocol & partner management	AVAILABLE	Matrix federation; partner management in admin.
Federation trust policy (cross-org enforcement)	ROADMAP	Federation Trust Policy (ADR-0028, D8).
E2EE for all classifications	PARTIAL	Currently enforced for the highest in-scope classification.
WORM archiving (compliance mode)	ROADMAP	Governance mode in preparation.
Encryption at rest (disk/DB/object)	ROADMAP	Phased improvement plan.
Highest classifications (secret/NATO/EU) electronic	ROADMAP	On-prem + HSM + accreditation process (see sec. 3/7).
Formal ISO 27001/27002 (BIO2) certification	ROADMAP	Not completed; open to discussion on request.



Implementation, pilot & scaling

- **Pilot model:** Wroote is looking for forward-thinking government organisations for a guided pilot, with early access, joint implementation and preferential terms when scaling to production.
- **Guided implementation:** from technical setup to user adoption.
- **Scaling:** the architecture is designed to grow from a single node to a multi-node, federated setup; the first phase targets large-scale use within central government.

Legal disclaimer & notice

This document is **informational** only and constitutes no offer, quotation or binding commitment within the meaning of contract law or procurement law. The content describes the state of the EuroChat platform as of the stated date (23 June 2026); features labelled **ROADMAP** or **PARTIAL** are not a guarantee and may change. No rights may be derived from this document.

Binding arrangements, including a data processing agreement (Art. 28 GDPR), service level agreement, security annex and any declaration of conformity, come about exclusively in a signed agreement. In a formal tender process, the tender documentation and the tender submitted in response always take precedence over this information pack. On request, Wroote provides additional, validated substantiation (architecture decisions, conformity dossier, security reporting) under confidentiality.

Contact

Pilot & procurement: pilot@wroote.eu

Privacy / data protection: privacy@wroote.eu

Web: wroote.eu