DEVELOPERS

Security evaluation package

This package describes how the Masnet integrations (webhooks and data API) protect company data. It is written for whoever assesses the risk of connecting Masnet to their systems. Anything not covered here is referred to the published legal documents.

Contract 1.7.0 (`sha256:18057f386936`), verified against the api-daas code at revision 5d30fed45e8f.

Scope and status

- It covers event delivery by webhook, the read data API and the events log, described in this documentation.
- Technical facts were verified against the platform code at revision `5d30fed45e8f` of api-daas; retention periods and design objectives come from the platform technical design and are marked as such.
- This package does not claim security certifications or third-party audits.
- Contractual terms (service level, sub-processors, data processing, vulnerability disclosure) are in the Complementary Annexes (published in Spanish) and the Privacy Policy; this page cites them and does not replace them.

Architecture and data flow

A business fact (for example, a contract changing status) is captured inside the same transaction of the business database and left in an outbox. A relay copies it into the events log, which lives in a separate database isolated per company. A single process, with no inbound access from the internet, takes the pending deliveries and sends them to the company HTTPS destination. That process is the only one with outbound internet access and the only one holding the private keys that decrypt destination credentials.

Event flow

```
Action in Masnet
  -> transactional capture (business database) -> outbox
  -> relay -> events log (isolated database, rows separated per company)
  -> delivery scheduler -> sender process (only one with internet egress)
  -> HTTPS (TLS) -> customer company destination
```

- Each delivery is projected, at send time, with the field groups the destination has been granted; before every attempt the state of the integration and of the destination and the current permissions are checked again.
- The API pods encrypt a destination credentials only with a public key: a compromised API can create material but cannot read it.
- An integration never administers integrations: its credentials cannot change the configuration.
- The data API is always limited to the company of the credential; the company is never a parameter and a foreign object responds as nonexistent.

Data that leaves, by domain and group

The company grants each integration a permission per domain and per field group. `public` and `business` leave when the domain is granted; `confidential` and `people` only with explicit confirmation from the administrator. The table counts, per object, the top-level fields of `data.object` that belong to each group according to the published schemas; a nested object counts as one field.

Object	Domain	public	business	confidential	people
`bid`	`bids`	1	13	0	0
`award`	`awards`	1	14	0	0
`contract`	`contracts`	3	18	0	0
`purchase_order`	`contracts`	4	11	0	0
`guarantee`	`guarantees`	1	20	0	0

Object	Domain	public	business	confidential	people
`opportunity`	`opportunities`	1	11	1	2
`tender`	`tenders`	11	2	0	0
`milestone`	`contracts`	0	11	0	0
`deadline`	`deadlines`	1	12	0	0
`audit`	`audit`	0	14	0	3
`document`	`documents`	0	4	0	2
`catalog_item`	`catalog`	0	21	3	0
`price_rule`	`prices`	0	6	12	0
`export`	`exports`	0	12	0	1
`communication`	`communications`	0	11	0	0
`survey`	`surveys`	0	11	0	0
`price_request`	`price_requests`	0	15	0	0
`framework_agreement_price_request`	`price_requests`	0	17	0	0
`client`	`clients`	1	16	0	1
`client_group`	`clients`	0	18	0	1
`sales_portfolio`	`sales_portfolios`	0	12	0	3
`sales_scope`	`sales_portfolios`	0	6	0	2
`client_assignment`	`sales_portfolios`	0	5	0	2
`product_group`	`catalog`	0	15	0	0
`competitor_mark`	`catalog`	2	12	0	2
`business_line`	`business_lines`	0	14	0	4

What is never exported

- Free text of comments, notes, conversations, justifications and internal remarks.
- File contents and signed URLs.
- KIM data, prompts and artificial intelligence answers.
- Personal marks (starred, followed, read, archived, discarded, flags, priority and folders), private tags and checklists, drafts and private tasks.
- Secrets and credentials, telemetry and navigation.

The user actions log exports the fact of each action, never its content. Name, email, IP and user agent additionally require the `people` group, and reading requires the administrator to declare that the company informed its users of the monitoring.

Encryption and signing

Surface	Mechanism
In transit	TLS. Design objective: TLS 1.2 as a minimum and TLS 1.3 preferred. Destinations must be HTTPS on port 443 or 8443.
Integrity and authenticity of deliveries	HMAC-SHA256 according to Standard Webhooks, with a per-destination secret generated by Masnet and shown only once. Rotation with two signatures for 24 hours.
Destination material at rest (URL, credentials and signing secrets)	Sealed envelope with X25519, HKDF-SHA256 and AES-256-GCM. Each part carries authenticated data that binds it to the company, the integration and the destination.
API client keys	Stored only as a SHA-256 hash and compared in constant time.
Access tokens	15-minute JWTs signed with a dedicated keyring, with key identifier, fixed issuer and audience, and rotation.

Network egress and IP addresses

Masnet does not publish fixed outbound IP addresses. Deliveries leave from addresses shared among companies, so the IP does not authenticate: the receiver must verify the signature or the credential. A receiver whose firewall requires a source IP allowlist uses pull mode (data API and event log), queried from its own network; if a company also requires receiving webhooks from known IP addresses, it is agreed with that company.

- Each attempt resolves the DNS name, rejects any non-public address and pins the connection to the validated addresses.
- Redirects are not followed and the response is read only up to 2 KiB.
- The address of the OAuth authorization server goes through the same defenses.
- The destination URL, which may include a signature in the query, is treated as a credential: it is encrypted, shown masked and not logged.

Retention

Values from the platform technical design:

Data	Retention
Events with their content (log and redelivery)	30 days
Deliveries, attempts and response excerpt	30 days
Deduplication marker	45 days
Configuration and permission audit	365 days
User actions log (read API)	365 days

Events are partitioned by day and deleted by partition. A request to erase personal data purges the affected content. For account data at the end of the contract, see section 9 of the Privacy Policy and Annex F.9 of the Annexes.

Audit

- Token issuance, authentication failures and reads of the events and actions logs are recorded per integration, with the request identifier.
- Ten authentication failures of a client within 15 minutes trigger a notice to the integration administrator. Repeated failures from one IP increase the delay and may block it; per client there is only delay, never blocking, so a third party cannot lock out a legitimate client.

- Configuration changes (destinations, permissions, credentials, declarations) are recorded and can be received as the `audit.integration_changed` event, which never includes secret values.
- Each delivery keeps its history: attempts, codes, duration and the SHA-256 digest of the body sent, to reconcile with the receiver.

Secrets management

- Signing secrets, API keys and client secrets are shown only once and cannot be read afterwards.
- API keys expire by default after 365 days and each client accepts two active secrets to rotate without interruption; revocation is immediate.
- Receiver response excerpts are sanitized: they do not retain the credentials that were sent to it.

Incident response

Published notification period: section 10 of the Privacy Policy states that, for security incidents affecting personal data, Masnet will assess the risk and notify the Customer or the affected data subjects within 72 hours of confirming the incident. Annex F.7 of the Annexes adds that notification is made without undue delay and with cooperation in the assessment. Vulnerability reports are sent to seguridad@masnet.com; the responsible disclosure policy is Annex B.

Sub-processors and data processing

- Roles: the customer company is the data controller and Masnet is the processor (Annex F.2).
- Sub-processors: Annex D describes their categories and obligations, and sections 7 and 8 of the Privacy Policy identify the providers and international transfers. Detailed information is provided on request at legal@masnet.com or privacidad@masnet.com.
- Law 21.719: the Privacy Policy describes the regulatory transition. For a detailed Data Processing Addendum, Annex F.10 says to request it from legal@masnet.com.
- Design measures of the integrations: minimization by default (`people` excluded), a record of every delivery, immediate revocation and bounded retention.
- Availability: Annex A sets the monthly availability of the Platform.

> This page does not replace the contractual documents. In case of any difference, the current Terms of Service, Privacy Policy and Annexes prevail.

External penetration test

The external penetration test prior to general availability **has not been performed yet**. Its results will be published on this page once it exists.