hoxey

PUBLIC

Data Processing Agreement

Article 28 GDPR terms for the Hoxey platform

DOCUMENT	VERSION	DATE	AUTHOR
ISMS-DPA-2026-001	1	2026-08-31	HOXEY S.r.l.s.

RFC 3161 timestamped · freetsa.org — verify in the signature panel

SUMMARY

The Article 28 terms on which Hoxey processes personal data for a customer, in either form: an Organisation using the platform for its own network, or a Partner operating it under its own brand within a dedicated tenant. Standard-form and unsigned, incorporated by the agreement under which the customer is engaged and identified there by version and digest. Annex 1 states the particulars of the processing, Annex 2 the technical and organisational measures.

CONTENTS

Preamble

This Data Processing Agreement ("DPA") contains the terms required by Article 28(3) of Regulation (EU) 2016/679 ("GDPR"). It applies between **HOXEY S.r.l.s.**, Via Stanislao Mattei 4, 40134 Bologna (BO), Italy, VAT and tax code 91478050379, REA BO-588294 ("Hoxey"), and the customer identified in the agreement, order, or activation email that incorporates it (the "Agreement"; that customer, the "Customer").

This DPA is a standard-form document. The parties are those identified in the Agreement, which is what makes this DPA binding. No separate signature is required.

Hoxey publishes this DPA at https://hoxey.io/legal/Hoxey-DPA.pdf, and the version published there applies. Each version is dated, superseded versions remain available, and the change history records the SHA-256 digest of the version each one supersedes.

Where a change would reduce the Customer's rights or Hoxey's obligations under this DPA, Hoxey gives the Customer at least thirty days' notice by email before it takes effect, and the Customer may object on the terms at clause 8. Any other change takes effect on publication.

The particulars of the processing are at Annex 1. The technical and organisational measures are at Annex 2. Both form part of this DPA.

1. Which form of Customer you are

The platform is supplied in two forms. The Agreement states which one applies. Read this clause first: the roles at clause 2 and the particulars at Annex 1 differ between them, and every other clause applies to both.

Organisation. The Customer uses the platform to protect its own network. Hoxey holds the Customer's user accounts, event records, and audit records.

Partner. The Customer operates the platform under its own brand for its own end customers, within a tenant dedicated to it. That tenant comprises a database instance in its own namespace, object storage holding its audit trail, and its configuration and secrets, held encrypted. The Partner's own contact email address and domain form part of that configuration. The Partner determines the tenant's contents. Hoxey does not access those contents in the ordinary course of providing the service; access occurs only where the Partner requests support, or where hosting operations require it.

Hosting that tenant is processing within the meaning of Article 4(2). Hoxey's obligations under this DPA apply to its contents in full, whether or not Hoxey has occasion to read them.

An end customer of a Partner is not a party to this DPA. Its relationship is with the Partner.

2. Roles

Where the Customer is an **Organisation**, the Customer is the controller and Hoxey the processor in respect of the personal data described at Annex 1.

Where the Customer is a **Partner**, the Partner is the controller in respect of its own account and users. In respect of its end customers' data, the Partner is the controller or, where it acts on their behalf, the processor, and Hoxey is processor or sub-processor accordingly. Hoxey holds and processes the contents of the Partner's tenant on the Partner's instructions and for no other purpose.

A Partner warrants that it has in place with each of its end customers the arrangements required by Article 28 in respect of the personal data it holds in its tenant, and that its instructions to Hoxey are instructions it is authorised to give. Hoxey is not responsible for the Partner's relationship with its end customers.

In either form, Hoxey is an independent controller in respect of the Customer's business contact, billing, and fiscal details. It processes them to perform and administer the Agreement, to correspond with the Customer, and to meet its accounting and tax obligations. The legal bases are performance of the contract and compliance with a legal obligation. The data is shared only with Hoxey's professional advisers and the providers identified in the sub-processor list referred to at Annex 1, and is stored within the European Union. Fiscal records are retained for the period Italian law requires; other records for the duration of the commercial relationship and a reasonable period thereafter. The individuals concerned may exercise their GDPR rights, or complain to the Garante, by contacting Hoxey at the address at Annex 1. This DPA does not apply to that processing.

Where the Customer is itself a processor acting for a third-party controller, references in this DPA to the Customer's instructions are to instructions the Customer is authorised to give.

3. Processing on documented instructions

Hoxey processes the personal data only on the Customer's documented instructions, including as regards transfers to a third country or an international organisation, unless required to do otherwise by Union or Member State law. Where such a requirement applies, Hoxey informs the Customer of it before processing, unless that law prohibits the information on important grounds of public interest.

The Agreement, this DPA, and the Customer's configuration and use of the platform constitute the Customer's documented instructions. Further instructions may be given in writing, and where they require Hoxey to do something the platform does not support, the parties will agree the terms on which it is done.

Hoxey immediately informs the Customer where, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection law.

Hoxey does not sell the personal data, does not use it to train models, and does not process it for its own purposes, save for the limited interest in the audit trail described at clause 13 and the derivation described at clause 4.

4. Derived threat intelligence

The honeypots operate within Hoxey's own infrastructure. Hoxey derives from decoy activity aggregate insight into attacker behaviour, including techniques, tooling, command patterns, and indicators of compromise, and uses it to improve the platform's detection capability and to contribute to the common security interest. This forms part of the service.

The derivation is performed within infrastructure Hoxey operates, as processing carried out on the Customer's instruction under this DPA. Material is extracted without the organisation or tenant identifier and without any other value identifying the Customer, a Partner, or their users. Addresses within the Customer's own network are not retained. Content supplied by an interacting party is redacted before use.

The extracted material is not personal data, and Hoxey's subsequent use of it falls outside this DPA. Nothing published or disclosed is attributable to a Customer, a Partner, an end customer, or an identifiable person.

Where the Agreement provides otherwise, the Agreement prevails.

5. The Customer's obligations

The Customer warrants that:

- it has a lawful basis for the processing it instructs, and its instructions comply with applicable data protection law;
- it has provided the information required by Articles 13 and 14 to the data subjects whose personal data it processes through the platform, including where applicable the individuals behind source addresses recorded in event records;
- the personal data it submits is accurate and lawfully obtained, and it does not itself submit special category data to the platform;
- it administers its own users, keeps credentials secure, and revokes access promptly when it is no longer required;
- where it determines that event records constitute Article 10 data under the law applicable to it, it is responsible for the condition required by that law, as stated at Annex 1; and
- where it is itself a processor acting for a third-party controller, it is authorised to give the instructions it gives.

6. Confidentiality

Hoxey ensures that every person authorised to process the personal data is bound by a written obligation of confidentiality that survives the end of their engagement, and that access is granted only to those who need it to perform the Agreement.

7. Security of processing

Hoxey implements the technical and organisational measures required by Article 32, having regard to the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to data subjects. Those measures are described at Annex 2 and apply to both forms of Customer.

Hoxey may vary the measures over time, provided the level of protection is not reduced. Annex 2 describes the platform as operated at the version date of this DPA.

8. Sub-processors

The Customer gives Hoxey general authorisation to engage the sub-processors identified in the list referred to at Annex 1.

Hoxey gives the Customer at least thirty days' notice by email before adding or replacing a sub-processor. The Customer may object on reasonable data protection grounds within that period, and the change does not take effect before that period has expired. The parties will discuss the objection in good faith, and where it cannot be resolved the Customer may terminate the Agreement in respect of the affected part of the service, or, where that part cannot reasonably be severed from the rest, the Agreement as a whole, without penalty and with a refund of any fee paid for a period not served.

Where the Customer objects within the notice period and the parties have not resolved the objection by its expiry, the change does not take effect while the discussion continues, save under the paragraph below.

Where continuity of the service requires Hoxey to move processing to an alternative infrastructure provider at short notice, including in response to an outage, incident, or loss of a provider, Hoxey may do so before the notice period has run, provided the alternative provider processes the personal data within the European Union and under measures affording a level of protection not lower than those at Annex 2. Hoxey notifies the Customer as soon as practicable and in any event within seventy-two hours, and the Customer's right to object under this clause then applies to the continued use of that provider.

Hoxey imposes on each sub-processor, by contract, data protection obligations equivalent to those in this DPA, and remains fully liable to the Customer for the performance of that sub-processor's obligations.

A Partner's own end customers are not sub-processors of Hoxey, and a Partner's own suppliers are the Partner's responsibility.

Payment processing is carried out by Stripe, Inc., which acts as an independent controller under its own terms in respect of the payment data it holds. That processing falls within the independent controller relationship described at clause 2 and outside this DPA, and Stripe is accordingly not a sub-processor under it. Hoxey does not receive card or payment method details.

9. International transfers

The personal data is stored within the European Union. The only routine processing outside the European Union arising from Hoxey's own arrangements is edge traffic handling by Cloudflare, Inc., which provides DNS, DDoS mitigation, web application firewall, and public TLS termination, and forwards the request to Hoxey's origin.

That transfer is covered by two independent bases. Cloudflare, Inc. participates in the EU-U.S. Data Privacy Framework. The standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, modules two and three as applicable, are also incorporated and in force between the parties, and continue to govern the transfer irrespective of the status of that Framework. Hoxey has carried out a transfer impact assessment in respect of that transfer and makes it available to the Customer on request.

Where the personal data is subject to the data protection law of a third country, the standard contractual clauses apply with the adaptations that law requires. In particular: where the Customer is established in Switzerland or the personal data is subject to the Swiss Federal Act on Data Protection, the standard contractual clauses apply with the adaptations recognised by the Federal Data Protection and Information Commissioner, so that references to the GDPR are read as references to the FADP, references to a supervisory authority include the FDPIC, and the clauses protect the data of legal entities where the FADP so requires; and where the Customer is established in the United Kingdom or the personal data is subject to the UK GDPR, the International Data Transfer Addendum issued by the Information Commissioner applies to the standard contractual clauses. In each case the Customer is the data exporter and Hoxey the data importer, and the courts and supervisory authority of the relevant jurisdiction apply in place of those named in the clauses. Where the Customer is established in another third country, the parties will agree the transfer mechanism required by the law applicable to it before processing begins.

Where the Customer configures a notification channel operated by a third party, Hoxey transmits the notification to that channel on the Customer's instruction. The operator of that channel is not a sub-processor of Hoxey, and Hoxey does not determine where it processes the data. Any transfer arising from that configuration, and the basis for it, are the Customer's responsibility.

Hoxey will not transfer the personal data to any other third country without first establishing a valid transfer mechanism and giving notice under clause 8.

10. Assistance with data subject rights

Taking into account the nature of the processing, Hoxey assists the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests to exercise rights under Chapter III of the GDPR.

The Customer administers its own users and has direct access through the platform to the account data and audit records within its own scope. A Partner administers its end customers and their users in the same way, within its own tenant. Access, rectification, and erasure are performed by the Customer directly. Where a request cannot be satisfied that way, Hoxey acts on the Customer's written instruction without undue delay.

Where a data subject addresses a request directly to Hoxey, Hoxey does not respond to it on its own account. It refers the data subject to the Customer and notifies the Customer promptly. Where the data subject is an end customer of a Partner, Hoxey refers them to that Partner.

11. Assistance with Articles 32 to 36

Taking into account the nature of the processing and the information available to it, Hoxey assists the Customer in ensuring compliance with the obligations at Articles 32 to 36, including security of processing, notification of a personal data breach, communication to data subjects, data protection impact assessment, and prior consultation with a supervisory authority.

Annex 2 and the Information Security Policy, available on request, support the Customer's data protection impact assessment.

Hoxey provides the assistance at clauses 10 and 11 at no charge where it is performed through the self-service functions of the platform. Where assistance requires material effort beyond that, Hoxey may charge on a time and materials basis at its then-current rates, notified to the Customer in advance and agreed before the work is undertaken. Hoxey does not charge for notification of a personal data breach under clause 12, or for any assistance where the need for it arises from Hoxey's own act or omission.

12. Personal data breach

Hoxey notifies the Customer of a personal data breach affecting personal data processed on the Customer's behalf without undue delay after becoming aware of it, and in any event within forty-eight hours. Hoxey becomes aware when it has a reasonable degree of certainty that a security incident has occurred that led to personal data being compromised.

The notification describes the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a point of contact, to the extent that information is available. Where it is not all available at once, it is provided in phases without further undue delay.

Where the Customer is a Partner, Hoxey notifies the Partner, and the Partner notifies its own end customers. Hoxey does not contact a Partner's end customers directly.

Hoxey does not notify a supervisory authority or a data subject on the Customer's behalf unless the Customer instructs it in writing to do so.

13. Retention, deletion and return

At the Customer's choice, Hoxey deletes or returns the personal data at the end of the provision of services, and deletes existing copies, unless Union or Member State law requires storage. The Customer may also request deletion at any time during the Agreement. Where the Customer is a Partner, this extends to the whole of the tenant dedicated to it.

The Customer makes its choice within thirty days of the end of the provision of services. Hoxey completes deletion within thirty days of that choice or, where no choice is made, within thirty days of the expiry of that period. Deletion is subject to the four retention characteristics below.

Where personal data is restored from backup following a disaster recovery event, Hoxey re-applies any deletion instruction given before the restore to the restored data without undue delay.

Four retention characteristics apply and are stated here:

- **Event records.** Event records are retained for ninety days from the date the event is recorded, and then deleted automatically.
- **Backups.** Database backups are immutable under object lock at the storage layer for thirty days and are deleted at thirty-five days. Deletion from the live system does not reach a backup already written. Backups serve disaster recovery alone and are never used to reconstitute data deleted from the live system.
- **Audit trail.** The audit trail records every action that changes state, including event ingestion and sensor health reporting. It is append-only and object-locked, so a deletion instruction does not reach records already written. It is retained for one year and then expires. Its immutability is a security measure Hoxey maintains under Article 32 and clause 7, and evidences compliance under Article 5(2). The trail is visible to the Customer through the platform within its own scope, and records the actions of Hoxey's own personnel, agents and system automation on the same terms as the Customer's: neither party can alter it, and each may rely on it against the other. It is used for no other purpose.
- **Operational telemetry.** Diagnostic logs are retained for fifteen days. They are used to operate and troubleshoot the platform, and for no other purpose.

Where the Agreement with a Partner ends, Hoxey retains the contents of the tenant dedicated to that Partner for thirty days before deletion, during which it acts on the Partner's instruction to return or transfer them. Where the Partner has ceased to operate and gives no instruction, Hoxey may, where it is lawful to do so and where it is able to identify the data concerned within the tenant, make an end customer's own data available to that end customer on its written request. Hoxey is

under no obligation to do so, and the Partner's arrangements with its end customers remain the Partner's responsibility.

14. Information and audit

Hoxey makes available to the Customer all information necessary to demonstrate compliance with Article 28 and allows for and contributes to audits, including inspections, conducted by the Customer or another auditor mandated by it. It does so in four ways:

- **Continuous independent verification.** The Customer has direct access, through the platform, to the append-only audit trail within its own scope. A Partner has that access across its own tenant.
- **The immutable record.** Where the Customer has reasonable ground to suspect that the record presented in the platform has been altered, Hoxey produces the corresponding object-locked copy from immutable storage for comparison.
- **Source code inspection.** The source code of the sensor deployed in the Customer's own network is available for inspection on request, including before any agreement is entered into.
- **Inherited certification.** Physical and environmental security is evidenced by the ISO/IEC 27001 certifications held by the hosting providers identified in the sub-processor list referred to at Annex 1, whose certificates and scope statements Hoxey provides on request.

Hoxey allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by it. The Customer gives thirty days' written notice, audits take place during business hours, and the Customer bears its own costs.

Physical and environmental security rests with the hosting providers identified in that list, to whom Hoxey will facilitate a request where an inspection of those premises is required. The parties expect the four mechanisms above ordinarily to discharge this clause. Where the Customer or a supervisory authority considers a further inspection necessary, Hoxey will agree its scope and conduct in good faith and will cooperate with any audit a supervisory authority requires.

Where the Customer mandates another auditor, Hoxey may require that auditor to be bound by confidentiality obligations no less protective than those in the Agreement, and may object to an auditor that is a competitor of Hoxey.

Hoxey maintains the records of processing required by Article 30(2) and provides the relevant extracts to the Customer on request.

Hoxey responds to a reasonable written request for information under this clause within thirty days. A request is satisfied where Hoxey provides its current Information Security Policy, the certification and scope statements of its hosting providers, and a written response to questions not addressed by them. Hoxey may decline a request that is repetitive or that seeks information already provided within the preceding twelve months. Audits and requests for information under this clause are each limited to once in any twelve-month period unless a personal data breach has occurred or a

supervisory authority requires otherwise. Information provided under this clause is Hoxey's confidential information, save that the Customer may disclose it to a supervisory authority or where disclosure is required by law.

15. Term

This DPA takes effect on the earlier of the Customer's acceptance of the Agreement and the commencement of processing, and continues for as long as Hoxey processes personal data on the Customer's behalf. Clauses 3, 6, 9, 12, 13 and 14 survive its termination for as long as Hoxey holds any of the personal data.

16. Precedence, liability and governing law

This DPA prevails over the Agreement in respect of data protection matters. The Agreement prevails in respect of commercial matters, including limitation of liability, service levels, governing law, and jurisdiction. The limitation of liability in the Agreement applies to claims arising under this DPA. Save for the notification period at clause 12, which binds Hoxey, nothing in this DPA creates a service level commitment.

Nothing in this DPA or the Agreement limits or excludes either party's liability toward a data subject under Article 82 GDPR, or any other liability that cannot be limited or excluded by law.

Where the Agreement is silent, this DPA is governed by Italian law, and the courts of Bologna have exclusive jurisdiction, save where a mandatory rule of law provides otherwise.

If a provision of this DPA is held invalid, the remainder continues in effect.

Annex 1: Particulars of the processing

Subject matter, nature and purpose

Provision of the Hoxey platform under the Agreement. The platform deploys honeypots within Hoxey's own infrastructure, receives from a sensor in the Customer's network the traffic directed to the decoy addresses that sensor presents, analyses that traffic for indications of attack, and reports the resulting security events to the Customer.

Hoxey processes personal data for these purposes only: hosting and administering the Customer's platform account, sending transactional email to the Customer's users, delivering event notifications to the channels the Customer configures, recording access and activity in the audit

trail, deriving aggregate threat intelligence as described at clause 4, and, where the Customer is a Partner, hosting and backing up the tenant dedicated to that Partner.

The sensor does not observe or capture traffic between other hosts on the Customer's network. Hoxey holds no payment or card details, no credentials to the Customer's systems, and no access into the Customer's network.

Duration

For as long as Hoxey processes personal data on the Customer's behalf under the Agreement, and thereafter for the retention periods stated at clause 13. Event records are retained for ninety days from the date of the event regardless of the duration of the Agreement, as stated at clause 13.

Categories of personal data

User account data (Organisation, Partner). Name, email address, role, and the notification channel identifiers configured by the user or by the Customer.

Audit records (Organisation, Partner). A record of every action that changes state, including event ingestion and sensor health reporting. Each captures the acting party and organisation as a snapshot at the time of the action, the affected resource, and the action taken.

Event records (Organisation, Partner). Structured records of interactions with a decoy, comprising the directed traffic reaching it and the activity performed on it, together with the source IP address and network metadata of the connection, the process and port identifiers involved, and the sensor output each record derives from. Where a device is deployed, its subnet.

The decoy-side fields describe the honeypot's own system. Hoxey observes a source IP as a network address only and holds no information of its own that links it to a person. An event record may also contain data supplied by the interacting party in the course of its activity on the decoy. Hoxey neither solicits nor controls that content, does not index or analyse it for any purpose beyond reporting the event to the Customer, and applies to it the retention period and measures stated for event records generally.

Operational telemetry (Organisation, Partner). Diagnostic and application logs generated in the course of operating the platform. Records reference users and organisations by internal identifier rather than by name, and may include an IP address. Retained fifteen days.

Partner-held data (Partner). The personal data held within the tenant dedicated to the Partner, across its database instance, its object storage, and its configuration. The Partner determines its categories, which ordinarily comprise those above in respect of the Partner's end customers.

Hoxey holds no documents, files, or content repositories on the Customer's behalf, and no derived analytics or profiles. The only IP addresses it holds are the source addresses in event records, retained ninety days, and those appearing in operational telemetry, retained fifteen days.

Hoxey does not solicit special categories of personal data within the meaning of Article 9, or personal data relating to criminal convictions and offences within the meaning of Article 10, and processes no such data for any purpose of its own. The Customer shall not itself submit special category data to the platform, and a Partner shall not permit its end customers to do so. Where such data reaches the platform through the activity of an interacting party on a decoy, Hoxey's processing of it is limited to what is stated in the event records entry above.

An event record describes activity observed on a decoy and is not an official finding of an offence. Hoxey's position is that such a record does not constitute Article 10 data. Where the Customer determines that it does under the law applicable to it, the Customer is responsible for the condition required by that law for the processing, and shall inform Hoxey.

Categories of data subject

- The Customer's personnel and other individuals whom the Customer authorises to use the platform.
- The individual behind a host that reached a decoy address, where the Customer is able to attribute the source IP to a person. Hoxey observes only the host's network address and cannot make that attribution; on an internal source address the Customer ordinarily can, from its own network records.
- Where the Customer is a Partner, the Partner's end customers and their personnel, and any other individual whose personal data is held within the tenant dedicated to the Partner.

Sub-processors

The current list of sub-processors, with their purpose, location, and transfer basis, is published at https://hoxey.io/legal/Hoxey-Sub-Processors.pdf and forms part of this Annex. Each version of that list is dated and retained, and superseded versions remain available.

Changes to that list are notified and may be objected to under clause 8. Publication does not constitute notice; notice is given by email as that clause provides.

The provider that delivers event notification email configured by the Customer, and transactional email to the Customer's users, also delivers Hoxey's own account and commercial correspondence. Hoxey is an independent controller in respect of that correspondence, which falls within clause 2 and outside this DPA.

Contact

Data protection enquiries: info@hoxey.io. Security and vulnerability reports: security@hoxey.io. Certified electronic mail: amministrazione@legal.hoxey.io.

Annex 2: Technical and organisational measures

The measures in force at the version date of this DPA. Their current implementation is described in Hoxey's Information Security Policy, available to the Customer on request. That document is informative and does not form part of this DPA. Hoxey may vary the implementation, provided the level of protection is not reduced.

Encryption in transit

Public traffic terminates TLS at the edge under a validated end-to-end configuration, with HTTP Strict Transport Security enforced. The edge terminates the session, which is what allows it to provide web application firewall and DDoS mitigation, and opens a second TLS session to the origin, which presents its own certificate. The personal data is therefore in plaintext only within the edge provider's own systems, which is why it is named as a sub-processor at Annex 1. No leg of the network path between the parties carries plaintext. Traffic between cluster nodes travels over an encrypted mesh.

Encryption at rest

Sensitive fields are encrypted at the application layer using AES-256 in an authenticated mode. Modification of a stored value is detected on decryption. Passwords are stored using a computationally expensive, salted hashing algorithm. The cluster's key-value store encrypts its secrets at rest independently.

Secrets and key management

Secrets reach version control only in sealed form, decryptable solely by the in-cluster controller holding the corresponding private key. Plaintext secrets are never committed. Operator credentials are held in a password manager, are decrypted into memory only for the duration of an active session, and are never persisted on a workstation. A secret sent to another party travels through an end-to-end encrypted link that expires on time or on a single retrieval. A secret that travels by any other route is rotated.

Identity and access

Identity is a three-level hierarchy of tenant, organisation, and user. Every data access is scoped server-side to the organisation identifier, and a client-supplied value cannot widen that scope.

Human sessions use a short-lived access token, a refresh token that rotates on each use, and a request-scoped token against cross-site request forgery. Multi-factor authentication is available to every account, and required for any account with administrative or critical access and for any Hoxey-held account able to reach customer data. Repeated failed attempts trigger lockout. Password reset is rate-limited and does not reveal whether an address holds an account.

Each automated link between components carries a distinct single-purpose credential scoped to one function. No component holds a general-purpose key to another.

Access is granted on least privilege and need to know. Account creation, role change, and deactivation are recorded in the audit trail.

Artificial intelligence

An AI assistant operated by Hoxey holds a dedicated, uniquely identified account on every system it touches, distinct from any human or machine-to-machine credential, and defaults to read-only. Write, execute, or configuration-changing capability requires a separate credential, not enabled by default, activated only for the task that requires it.

No AI assistant account is granted access to secrets or credentials, regardless of what access is otherwise available to it.

Where an AI assistant operated by Hoxey reaches personal data processed on the Customer's behalf, one of the following applies:

- the data is processed wholly within infrastructure Hoxey operates; or
- the data is pseudonymised before it leaves infrastructure Hoxey operates. All identifying values are replaced by substitutes, by tokenisation, encryption under a locally held key, or an equivalent method, including IP addresses and any identifier appearing in party-supplied content. The information needed to reverse the substitution is held only within infrastructure Hoxey operates and is never transmitted, and reversal occurs only within it. The provider receives no means by which an individual could be identified.

Actions taken by an AI assistant account against the management interface are recorded in the audit trail in the same way as those of a human.

Security operations are decided and actioned by a human.

Where the Customer connects an AI agent to the platform's programmatic interface, that is the Customer's own processing decision, under its own responsibility, and the provider of that agent is not a sub-processor of Hoxey.

Segregation

Each tenant occupies its own namespace, with its own database and credentials. Cross-namespace access is granted by explicit policy naming the source namespace by label and the source workload by name. No policy admits one tenant's workloads to another tenant's namespace or data stores. Organisations within a tenant are segregated by the server-side scoping above.

Network isolation

Successive layers separate a public request from a workload: the edge provider, a single public ingress address bound to one node, an encrypted node mesh, and cluster-internal services. At the ingress, TLS terminates with an origin certificate behind an allowlist restricted to the edge provider's published address ranges. Administrative shell access and the cluster API server are restricted to named source addresses. Access between workloads is granted by explicit policy naming source, destination, and port, with default deny for any workload so selected.

Architecture

Data flows in one direction between the sensor and Hoxey's infrastructure. The sensor initiates every exchange, and Hoxey holds no route, credential, or listening endpoint by which a connection into the Customer's network could be opened. Components are mutually distrusting. Application containers run with a read-only root filesystem, with writable paths only where explicitly declared.

Runtime self-protection

Every application runs a purpose-built in-process monitor that detects operations the application never performs in the course of its normal function. Any occurrence is treated as compromise. The monitor is custom to the platform, produces no false positives in normal operation, and is not documented externally. It is the control by which code execution is made non-viable: a vulnerability in the application, or a compromised dependency, does not by itself yield a usable execution path. The monitor runs in production and is armed inside the automated test suite, where a violation fails the build.

Logging, audit and monitoring

A dedicated audit trail records security-relevant actions taken through the management interface. Records are append-only, and none is updated or deleted once written. Each captures the acting party and organisation as a snapshot at the time of the action, the affected resource, and a structured description of the action. Retention is one year under object lock in compliance mode. The trail is visible to the Customer through the platform, scoped to role and organisation.

Secure development and change control

Every change to a production application passes through a pull request, reviewed and approved before merge, and subject to static supply-chain vetting of any dependency it introduces. The full automated test suite runs against the merge commit ahead of the image build. A dependency vulnerability audit gates the build and fails where an advisory is reported against a shipped dependency. A triaged advisory is muted individually by identifier, with its category, justification, and review date recorded.

Every externally reachable endpoint validates its input against an explicit schema. Database access at the application layer is exclusively through an object-relational mapping layer. Testing is comprehensive and adversarial in design, aimed at breaking the application rather than confirming its behaviour, and is gated in the build.

Production deployment of application workloads is driven from version control, and a reconciliation process continuously corrects drift. A small number of platform components are installed once at cluster creation and thereafter managed under the same declarative model. Development and staging environments are structurally separate from production.

Resilience, backup and recovery

Recovery point is bounded by continuous transaction log archiving with periodic full backups, and is ordinarily a matter of minutes. Recovery is driven from infrastructure as code with no dependency on a particular provider, and is tested. These describe the design of the platform. They are not a service level, and any service level commitment is a matter for the Agreement.

Three independent backup streams run continuously, each stored off-cluster: database backups combining continuous log archiving with periodic full backups, cluster state snapshots at short intervals, and operational log archives. Database backups are held under object-lock immutability in compliance mode for thirty days, during which no deletion or alteration is possible regardless of which credentials or systems are compromised, including the backup software.

The platform is defined declaratively in version control and can be reconstructed from that declaration.

Nodes are scheduled across separate physical hosts, and backup storage is held in a different region from the compute it protects.

Personnel

Access that reaches customer data, or information classified Confidential or above, is granted only against a signed confidentiality agreement that survives the end of the engagement. Access is revoked immediately at the end of an engagement. Access to customer data is held by named individuals and is reviewed on change of role.

Governance

Hoxey operates an information security management system aligned to ISO/IEC 27001:2022, with a documented scope, risk assessment, risk treatment plan, statement of applicability, and a documented set of binding rules. Certification is planned; Hoxey does not represent itself as certified. The Information Security Policy is available to the Customer on request.

Change history

Each row records the SHA-256 digest of the version it supersedes, so the sequence of published versions can be verified against the files themselves.

Version	Date	Summary of change	SHA-256 of the superseded version
1.0	2026-08-31	First published version.	None