CRYPTAGION — Security Posture

Document scope: the technical, organisational, and contractual measures that govern CRYPTAGION's handling of customer source code, certificates, and derived artefacts during a 60-day pilot or standard discovery engagement. This document is intended for inclusion in the customer's vendor security file.

1. Service overview

Provider	KOR IT SASU — registered in Paris, France (RCS Paris)
Service	CRYPTAGION cryptographic discovery — 60-day fixed-fee engagement
Delivery model	Service engagement; no CRYPTAGION software is installed on customer infrastructure during the pilot
Data classification	Customer source code is treated as "Confidential — Customer IP" throughout

2. Processing infrastructure

Hosting provider	OVH SAS (`ovhcloud.com`)
Region	Gravelines, France (`eu-west-gra`) — EU territory, GDPR jurisdiction
Hardware	OVH Kimsufi KS-7 dedicated bare-metal server · AMD EPYC 7451 (24 cores) · 256 GB ECC RAM · 2× 500 GB NVMe SSD with software RAID-1
Hypervisor	Proxmox Virtual Environment 9
Per-customer isolation	Each engagement is allocated a dedicated Proxmox VM. VMs are not shared between customers under any circumstance.
Provider certifications	OVH is ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018, and SecNumCloud certified (verify at https://corporate.ovhcloud.com/en/sustainability/certifications/)

The CRYPTAGION processing infrastructure is **physically located in France** and is owned and operated exclusively by KOR IT SASU on hardware leased from OVH SAS. No customer data is

replicated to, transferred to, or processed by infrastructure outside the European Economic Area at any point in the engagement lifecycle.

3. Access control

LAYER	CONTROL
Host (Proxmox)	SSH public-key authentication only; password authentication disabled. UFW firewall with deny-by-default ingress; only ports 22 (SSH) and 8006 (Proxmox UI) exposed. Fail2ban enabled.
Customer VM	Each VM has SSH public-key authentication. Only the engagement lead (Ali Korsi) holds SSH keys to customer VMs.
Sudo / root	Customer VMs are administered as root by the engagement lead only. There are no shared credentials.
2FA	The Proxmox web UI account is protected by TOTP two-factor authentication.
Audit log	All VM provisioning and destruction operations are recorded to `/var/log/cryptagion/customers.tsv` with timestamp, VM ID, customer slug. Retained for 90 days per GDPR Article 30.

4. Customer data lifecycle

4.1 Ingress (how customer code reaches CRYPTAGION)

The customer chooses the access pattern; the engagement lead does not select unilaterally. Three options ranked in customer-preference order:

OPTION	MECHANISM	CUSTOMER RETAINS CONTROL VIA
A · Deploy-key on customer mirror *(preferred)*	Customer creates a read-only mirror of in-scope repositories on a dedicated VCS organisation; grants a deploy key.	Revoking the deploy key at engagement end; full audit trail in customer's VCS
B · Customer-side ephemeral clone	Customer clones into an isolated location and grants one-time SFTP credentials to the engagement VM.	One-time credentials with built-in expiry
C · Live screen-share scan	The scan is executed during a screen-share session; the customer watches each command.	Direct supervision of every operation

For all three options: **CRYPTAGION's code itself is not installed on customer infrastructure during the discovery engagement**. There is no agent, no daemon, no scheduled job running on customer-owned systems.

4.2 Processing

The customer VM holds: - A working clone of the customer's repository (for the duration of the scan) - A SQLite database (`cryptagion.db`) containing the asset inventory - Generated deliverables (CycloneDX CBOM JSON, PDF executive report, migration roadmap JSON) - No customer code, secrets, credentials, or personal data are transmitted outside the customer VM at any point.

4.3 Egress (how deliverables reach the customer)

Deliverables are pushed to a customer-specified destination — typically a customer-owned SFTP server, git repository, or object-storage bucket — under the customer's identity and credentials. Deliverables are signed with SHA-256 checksums for integrity verification.

4.4 Destruction

Within 7 days of engagement closure (typically same day as the final walkthrough):

1. The customer VM is shut down and irrevocably destroyed via `qm destroy --purge --destroy-unreferenced-disks` . This de-allocates the virtual disk from the Proxmox storage pool, overwriting its blocks.
2. A **data destruction certificate** is automatically generated and emailed to the customer's nominated compliance contact. The certificate identifies the VM, the storage backend, and the destruction timestamp under signature of the engagement lead.
3. The audit log entry is updated with the destruction timestamp.
4. **What KOR IT retains** (per GDPR Article 30 retention obligations):
5. The destruction certificate itself (perpetual)
6. The audit-log row for this engagement (90 days)
7. Any deliverable artefact the customer explicitly elected to retain for KOR IT's records (e.g. for use as a case-study reference under separate signed agreement)

5. Encryption

AT REST	IN TRANSIT
Customer VM disks reside on Proxmox `local-lvm` storage. The Proxmox host's NVMe disks support hardware encryption via OPAL. Customer VMs can additionally use LUKS full-disk encryption on request; this is the default for engagements involving regulated personal data.	All ingress (SSH, SFTP) uses modern TLS / SSH cipher suites: AES-256-GCM, ChaCha20-Poly1305. Legacy ciphers (3DES, RC4, MD5, SHA-1) are disabled in `/etc/ssh/sshd_config` and the OVH-managed firewall.

6. Vulnerability + patch management

- Proxmox host runs `unattended-upgrades` for Debian security updates daily.
- Customer VMs are cloned from a template that is patched to current Debian stable releases at provisioning time.
- CRYPTAGION dependencies are pinned in `pyproject.toml` and reviewed at every release; `uv lock` ensures reproducible installs.
- Quarterly third-party vulnerability scan against the Proxmox host (TrivyScan / Nuclei).

7. Personnel

Personnel with customer-data access	Ali Korsi (Founder, KOR IT SASU). Background check on request.
Sub-processors	OVH SAS (infrastructure provider — see §2). No other sub-processors.
Personnel changes	Customers will be notified in writing within 5 business days of any change in personnel with access to their data.

8. Contractual envelope

Every engagement is governed by three documents, signed before any technical work begins:

DOCUMENT	PURPOSE
Mutual NDA	Perpetual confidentiality obligation on customer source, business information, and engagement findings.
Statement of Work (SOW)	Scope, deliverables, timeline, fees, IP ownership (deliverables = customer property; CRYPTAGION tool = KOR IT IP), liability cap (typically 1× engagement fees), warranty.
Data Processing Agreement (DPA)	GDPR Article 28 compliance. KOR IT is processor; customer is controller. Specifies categories of data, processing purposes, sub-processors (OVH only), assistance with data-subject rights, sub-processor change notification, breach notification (within 48h to the customer's DPO).

Standard templates are available on request prior to commercial engagement.

9. Incident response

Breach notification window	KOR IT will notify the customer's DPO (or named security contact) within **48 hours** of becoming aware of any incident reasonably suspected to involve customer data.
Communication channel	The contact named in the DPA's "Notice" clause, by email + phone.
Incident response coordination	KOR IT will participate in the customer's incident-response process and provide all reasonable assistance, including forensic imaging of the affected VM where applicable.
Public communications	Any public statement by KOR IT referencing an incident touching customer data requires prior written approval from the customer.

10. Documentation references

- **Methodology citations** — risk scoring weights are documented in code at `src/cryptagion/risk/scorer.py`, anchored to NIST IR 8413, NIST SP 800-131A Rev. 2, BSI TR-02102-1 (2024 revision), and NSA CNSA 2.0.
- **CBOM specification** — CycloneDX 1.6 (https://cyclonedx.org/docs/1.6/json/).
- **Validation** — CBOM output is verified against the official CycloneDX 1.6 strict JSON schema before delivery to the customer.

11. Contact

ROLE	CONTACT
Engagement lead / commercial	Ali Korsi — `contact@cryptagion.io`
Security incidents	`contact@cryptagion.io` (subject: `[SECURITY]`)
Data subject rights	Per Article 13 GDPR — `contact@cryptagion.io` (subject: `[DPA]`)

This document is provided for the customer's information-security file and does not modify the contractual obligations specified in the signed NDA, SOW, or DPA. Where this document and the signed contractual documents differ, the signed documents prevail.

— KOR IT SASU · Paris, France · cryptagion.io