OST Labs
Security & Data Protection Whitepaper

How OST Labs protects customer data across its Atlassian Marketplace and monday.com apps.

Built on Forge • **Cloud Fortified** • **Bug Bounty** • **EU Data Residency** • **GDPR**

Publisher: OST Consulting SRL (OST Labs), Belgium • VAT BE 0741 577 074
Version 1.1 • Effective 25 June 2026
Contact: info@ost-consulting.be

Contents

1. Executive summary

OST Labs (OST Consulting SRL) is a Belgium-based software company building apps for Atlassian Jira, Atlassian Confluence and monday.com, distributed through the Atlassian Marketplace and the monday.com Apps Marketplace. Security and data protection are owned at company level and built into how every app is designed, hosted and operated.

This whitepaper summarises our security posture for technical and procurement reviewers. In brief:

- Every Atlassian app is built on Atlassian Forge. Smart Label Manager runs entirely on Atlassian infrastructure (Runs on Atlassian); the other apps use a Forge remote backend hosted in the European Union.
- All vendor-hosted data resides in the EU (DigitalOcean, Frankfurt, Germany).
- Data is encrypted in transit (HTTPS/TLS) and at rest (AES-256).
- Process Templates, Easy Clone and HTML Macro Pro hold the Atlassian Cloud Fortified badge.
- We participate in the Atlassian Marketplace Security Bug Bounty Program on Bugcrowd and remediate vulnerabilities to Atlassian's published timelines.
- We are GDPR-aligned, operate under Belgian and EU law, and make a Data Processing Agreement available to customers.

OST Labs does not currently hold a SOC 2 or ISO 27001 certification. This document, together with our Cloud Fortified status, Bug Bounty participation and published controls, is intended to give reviewers the assurance they need.

2. Our apps and architecture

OST Labs publishes the following apps. Their hosting model differs, so we state it explicitly per app. “Forge remote backend” means the app is built on Atlassian Forge but calls a backend service we operate in the EU; data processed by that backend leaves Atlassian's cloud for our EU infrastructure.

App	Platform	Hosting model	Where data lives	Badge
Smart Label Manager	Jira	Pure Forge, no remote backend	Stays in Atlassian's cloud	Runs on Atlassian
Process Templates for Jira	Jira	Forge + EU remote backend	DigitalOcean, Frankfurt (EU)	Cloud Fortified
Easy Clone for Jira	Jira	Forge + EU remote backend	DigitalOcean, Frankfurt (EU)	Cloud Fortified
HTML Macro Pro	Confluence	Forge + EU remote backend	In transit via EU backend; not stored	Cloud Fortified
Calendar Embed & Sync	monday.com	monday platform + EU backend	DigitalOcean (EU)	n/a

Because the apps are built on Forge, they inherit the security properties of the Atlassian platform: manifest-declared permission scopes, Atlassian-managed authentication and tenancy, and (for the pure-Forge app) data residency without any external storage.

3. What data we process and where

By design, our apps process the minimum data needed to deliver their function. Most customer content remains inside the Atlassian or monday.com platform; only the data described below is handled by our EU backend.

App	Data handled by our backend	Retention
Smart Label Manager	None stored outside Atlassian; operates within the Jira instance	n/a (no external storage)
Process Templates	Template definitions and configuration	Stored while the app is subscribed; removed on uninstall/request
Easy Clone	Issue data processed transiently to run a clone job	Not stored; processed transiently
HTML Macro Pro	Macro content processed in transit only, to operate the secure sandbox	Not stored; processed transiently
Calendar Embed & Sync	Calendar and event metadata for embedding and sync	Stored while the app is subscribed; removed on uninstall/request

Across all apps we also process limited technical and operational data (for example log data and de-identified diagnostics) to keep the apps reliable and secure, as described in our customer agreement and Privacy Policy.

4. Data residency

All data persisted or processed by OST Labs backends is hosted in the European Union, in DigitalOcean's Frankfurt (Germany) region. Smart Label Manager stores no data outside Atlassian, so its data residency follows the customer's Atlassian

instance. Changing an Atlassian instance region does not automatically migrate data already held by an app; contact us if a specific residency arrangement is required.

5. Encryption and key management

OST Labs follows generally accepted industry practices to protect data:

- In transit: all connections use HTTPS/TLS.
- At rest: data is encrypted using AES-256.
- Secrets and access tokens are protected and accessible only to the application, not to support staff in plaintext.
- Encryption keys are managed by the underlying cloud platform's key-management services.

6. Application security

Our apps are built on Atlassian Forge and follow Atlassian's security requirements for Marketplace apps:

- Least-privilege permission scopes, declared in the Forge manifest and reviewed at each release.
- Secure development practices, including code review and dependency management.
- Participation in the Atlassian Marketplace Security Bug Bounty Program, hosted on Bugcrowd, providing continuous independent testing.
- Cloud Fortified status for Process Templates, Easy Clone and HTML Macro Pro, which requires meeting Atlassian's combined security, reliability and support criteria.

7. Infrastructure and operational security

Our EU backend runs on DigitalOcean (Frankfurt). Physical and environmental security of the data centres is provided and independently audited by the cloud provider. At the application and operational layer we maintain:

- Network segmentation between public-facing and private components.
- Backups with restore procedures for persisted data.
- Monitoring and logging of system activity, including error monitoring.
- Controlled deployment through a reviewed release process.

8. Access control

OST Labs personnel access customer data only when strictly necessary to provide support or maintenance, and such access is logged and monitored. Administrative access to production systems is restricted, protected by multi-factor authentication, and limited to authorised personnel. Customers are responsible for safeguarding their own accounts and credentials used to access the host platforms.

9. Subprocessors

OST Labs keeps its subprocessor footprint deliberately minimal. Under GDPR Article 28, a subprocessor is a third party that processes customer personal data on our behalf. We engage the following:

Subprocessor	Role	Data location	Applies to
DigitalOcean	Application backend hosting and storage	Frankfurt, Germany (EU)	Apps with a backend (Process Templates, Easy Clone, HTML Macro Pro, Calendar Embed & Sync)
Cloudflare	Edge network and web application firewall (WAF): TLS termination, CDN and DDoS protection; processes traffic in transit	Global edge network (US-headquartered; EU localisation available)	The website and the apps with an EU backend
Atlassian	Customer support helpdesk (Jira Service Management), where support communications are processed; and the Forge platform that runs the apps	EU (per Atlassian data residency)	Support, and all Atlassian apps

Platforms and tooling, for clarity:

- monday.com is the host platform for the Calendar Embed & Sync app, which the customer contracts with directly.
- Smart Label Manager stores no customer data outside Atlassian and engages no backend storage subprocessor.
- Error monitoring is performed on de-identified diagnostic data only. No customer personal data is sent to it, so it is not a data subprocessor.
- Where a subprocessor operates outside the EEA (such as Cloudflare's global edge), transfers are covered by EU Standard Contractual Clauses and the provider's data processing terms.

We will provide notice of material changes to our subprocessors in line with our Data Processing Agreement.

10. Vulnerability management and incident response

We accept vulnerability reports through our support helpdesk (ost-consulting.atlassian.net) and through our Bugcrowd bug bounty program. We remediate confirmed vulnerabilities in line with the Atlassian Marketplace Security Bug Fix Policy timeframes for cloud apps:

Severity	CVSS	Remediation due (cloud apps)
Critical	≥ 9.0	Within 10 days of report or triage
High	≥ 7.0	Within 4 weeks
Medium	≥ 4.0	Within 12 weeks
Low	< 4.0	Within 25 weeks

Vulnerabilities reported through the bug bounty have a two-week triage window before the remediation clock begins. If we become aware of an incident that compromises the security of your data, we will notify you without undue delay with the information reasonably available at the time.

11. Compliance and certifications

- Cloud Fortified (Atlassian) for Process Templates, Easy Clone and HTML Macro Pro.
- Runs on Atlassian for Smart Label Manager.
- Atlassian Marketplace Security Bug Bounty Program participant (Bugcrowd).
- GDPR-aligned; Data Processing Agreement available on request.

OST Labs does not currently hold SOC 2 Type II or ISO 27001. Our controls are aligned with recognised industry practice, and we can complete customer security questionnaires (including CSA CAIQ-Lite) on request.

12. Legal, data subject rights and retention

Our apps are governed by our customer agreement and Privacy Policy, under Belgian and EU law (OST Consulting SRL, VAT BE 0741 577 074). Customers may exercise GDPR data-subject rights by contacting us. App data held on our backend is removed within 10 business days of the app being uninstalled or the subscription ending (the cessation date), or earlier on request, subject to short operational backup cycles. This deletion window matches the commitment in our Data Processing Agreement.

13. Contact

Security and privacy enquiries: info@ost-consulting.be

Support: ost-consulting.atlassian.net (helpdesk)

To request the Data Processing Agreement or a completed CAIQ-Lite, email info@ost-consulting.be. To report a vulnerability, use our support helpdesk (ost-consulting.atlassian.net) or our Bugcrowd bug bounty program.

This document is provided for information and does not modify our customer agreement or Privacy Policy. In case of conflict, those agreements prevail.

Version history. v1.1 (25 June 2026): added Cloudflare as a subprocessor (edge network and WAF) and a cross-border transfer note; vulnerability reports now routed through the support helpdesk. v1.0 (20 June 2026): first release.