Sicherheit & Datenschutz

Whitepaper zur MSGI-Automatisierungsplattform (n8n)

Gehostet in der EU (Frankreich) · DSGVO-konform · isolierte Umgebungen

Dieses Dokument beschreibt die Sicherheits- und Datenschutz-Architektur der MSGI-Plattform, über die Kunden fertige Automatisierungen (n8n-Workflows) in ihrer eigenen, isolierten Umgebung betreiben. Es richtet sich an Entscheider, IT- und Sicherheitsverantwortliche.

Hosting	EU (Frankreich), DSGVO-konform
Isolation	Eigener Container + Datenbank + Verschlüsselungs-Key je Kunde
Transport	TLS (Let's Encrypt), HSTS erzwungen
Zugriff	Rollen Owner/Editor/Viewer, Einladung per E-Mail
Backups	Verschlüsselt, nächtlich, offsite, Restore-getestet
Stand	02.07.2026

Live-Sicherheitsseite: https://flows.msg-i.de/security · Kontakt: flows@msg-i.de

1. Zusammenfassung für Entscheider

Die Plattform ist auf Datensouveränität und Mandantentrennung ausgelegt. Jeder Kunde erhält eine vollständig isolierte Automatisierungsumgebung in der EU (Frankreich). Zugriff ist rollenbasiert, alle sicherheitsrelevanten Aktionen sind protokolliert, und Daten werden verschlüsselt gesichert. Der folgende Bericht beschreibt die konkreten Maßnahmen – ohne Marketing-Floskeln.

2. Hosting & Datensouveränität

- **100 % in der EU** gehostet (IONOS, Frankreich) – Daten verlassen die EU nicht.
- **DSGVO-konform** durch EU-Hosting und Datenminimierung; Auftragsverarbeitungsvertrag (AVV) auf Anfrage.
- Verschlüsselte Übertragung: **TLS** mit gültigen Let's-Encrypt-Zertifikaten, **HSTS** erzwungen.
- Kein Vendor-Lock-in: Basis ist das offene n8n; Workflows sind exportierbar.

3. Mandanten-Isolation

- **Eigener Container pro Kunde** – kein geteilter Automatisierungs-Server.
- **Eigene Datenbank** je Kunde, in einem internen Netz **ohne Internet-Zugang**.
- **Eigener Verschlüsselungs-Key** je Umgebung für gespeicherte Zugangsdaten.
- **Netzwerk-Isolation**: Kundenumgebungen können sich gegenseitig nicht erreichen (Ost-West-Isolation).

4. Zugriffskontrolle & Rollen

- Rollen je Umgebung: **Owner** (volle Kontrolle), **Editor** (bearbeiten), **Viewer** (nur lesen).
- **Viewer sind streng schreibgeschützt**: kein Zugriff auf den Live-Editor oder auf Zugangsdaten – sie sehen nur eine strukturierte, bereinigte Diagramm-Ansicht (ohne Parameter/Secrets).
- Mitglieder werden per E-Mail eingeladen; Beitritt nur mit der eingeladenen Adresse.
- Rollen werden serverseitig erzwungen (nicht nur im UI ausgeblendet).

5. Authentifizierung & Konten

- Passwörter mit **PBKDF2** (200.000 Iterationen) gehasht – niemals im Klartext gespeichert.
- Durchgesetzte **Passwort-Richtlinie**: min. 10 Zeichen, Groß-/Kleinbuchstabe, Ziffer, Sonderzeichen, Sperrliste gängiger Passwörter, kein Name/E-Mail-Bezug.
- **E-Mail-Bestätigung** bei Registrierung; Passwort-Reset über zeitlich begrenzte, signierte Links.
- Sitzungen über signierte, HttpOnly-Cookies.

6. Nachvollziehbarkeit (Audit-Log)

- **Manipulationsarmes, append-only Protokoll** aller sicherheitsrelevanten Aktionen (Login mit IP, Rollen-/Mitgliederänderungen, Workflow-Änderungen, Schlüssel-Rotation u. a.).
- Umgebungs-Owner sehen das Protokoll ihrer eigenen Umgebung; Betreiber-Admins eine globale Sicht.
- Export als CSV für eigene Aufbewahrung/Reviews.

7. Betrieb, Backups & Wiederherstellung

- **Verschlüsselte, nächtliche Backups** (restic) an einen separaten Offsite-Speicher – Wiederherstellung getestet.
- Aufbewahrung nach Generationen-Prinzip (täglich/wöchentlich/monatlich).

- **Monitoring** des Plattform- und Umgebungszustands; öffentliche Statusseite unter /status.
- Selbst-Service für Kunden: Umgebung neu starten, Zugriffsschlüssel rotieren.

8. Infrastruktur- & Betriebssicherheit

- Verwaltungs-Zugriff auf die Container-Ebene nur über einen **gefilterten Socket-Proxy** – kein direkter Docker-Socket.
- Container laufen mit **no-new-privileges** und Ressourcen-Limits.
- Interne API-Dokumentation (Swagger/OpenAPI) ist in Produktion **deaktiviert**.
- Security-Header (HSTS, X-Content-Type-Options, Referrer-Policy) auf den Portal-Endpunkten.

9. Datenschutz & Compliance

- Verarbeitung in der EU (Frankreich); Datenminimierung by Design.
- Auftragsverarbeitungsvertrag (AVV/DPA) sowie ein Verzeichnis der Verarbeitungstätigkeiten auf Anfrage.
- Löschkonzept: Kundendaten werden mit der Umgebung entfernt (Deprovisionierung inkl. Datenbank).

10. Verantwortungsvolle Offenlegung

Sicherheitsmeldungen bitte vertraulich an **flows@msg-i.de**. Wir bestätigen den Eingang, halten Melder auf dem Laufenden und bitten um angemessene Zeit zur Behebung vor einer Veröffentlichung.

11. Aktueller Stand & Ausblick (Transparenz)

Wir kommunizieren offen, was noch im Aufbau ist:

- Bezahl-/Abo-Funktionen und Nutzungslimits werden derzeit ergänzt.
- Erweitertes Monitoring mit Benachrichtigungen (Uptime/Alerting) wird ausgerollt.
- Personenscharfe Rechte *innerhalb* der n8n-Editoransicht (über die Portal-Rollen hinaus) sind ein geplanter, weitergehender Schritt.

Dieses Whitepaper beschreibt den Stand zum angegebenen Datum und ersetzt keine vertragliche Zusicherung. Aktuelle Informationen: https://flows.msg-i.de/security und /status. Kontakt: flows@msg-i.de.