European Union GDPR/DORA/NIS2 summary

Processor and ICT third-party inputs for EU buyers

Trustholm - European Union GDPR / DORA / NIS2 vendor pack (summary)

Use with

- - /compliance/eu/gdpr-processor-framing
- - /compliance/eu/dora-ict-risk
- - /compliance/eu/nis2-msp-ict-supply-chain
- - /resources/digital-sovereignty-eu-msp-saas

Trustholm does NOT claim "GDPR compliant product", DORA certification, or NIS2 certification badges.

VENDOR ORIGIN

- - Product: Trustholm (policy and evidence engine for MSP privileged automation)
- - Global legal entity: Trustholm Pty Ltd (Australia)
- - Leadership: European Union (EEA) founder-led vendor
- - EU/EEA contracting: Entity and VAT details confirmed during enterprise onboarding
- - EU procurement contact: security@trustholm.com (CET/CEST business hours)

US STACK vs TRUSTHOLM ROLE (complement positioning)

| Layer | Typical US vendor | Trustholm role | |---|---|---| | Patch / inventory | NinjaOne, ConnectWise | Not replaced - customer keeps incumbent | | Remote monitoring | US RMM | Not replaced | | Script governance | Often same US RMM | Signed policy, approval, audit export | | Agentic automation | US agentic platforms | Execution-intent gate + attestation | | Audit evidence | Operational RMM logs | Security audit plane + export APIs |

Pragmatic EU sovereignty: reduce single-vendor dependency for privileged automation proof.

DEPLOYMENT OPTIONS (data plane)

1. Shared multi-tenant SaaS - EU region (api-eu / portal-eu) for pilot and GA tenants 2. DedicatedDatabase - separate Postgres instance per tenant 3. Self-hosted / air-gapped (Enterprise bundle) - customer-operated infrastructure

Production launch region: Australia. EU home region available via enterprise onboarding. Marketing site (www) uses US Vercel edge - trial forms only, no tenant production data.

SUBPROCESSOR GEOGRAPHY (summary)

- - Tenant production: Regional cloud (AU launch; EU available) - see /trust/subprocessors
- - Marketing / trial signup: US (Vercel), optional US Mailchimp, Cloudflare global
- - Transactional email: Configured per deployment
- - Analytics (www only): US Google Analytics (consent-gated)

Request live subprocessors list at /trust/subprocessors before DPIA finalization.

GDPR (typical processor role)

- - Subprocessors list published at /trust/subprocessors
- - DPA negotiated at enterprise onboarding
- - Article 32 measures: isolation, MFA, audit export, signing policy
- - Subject rights: controller-operated programs; export within tenant scope
- - Cross-border transfers: SCCs and schedules in enterprise DPA

DORA (financial sector ICT third-party)

- - Register inputs: architecture overview, questionnaire pre-fill, subprocessors
- - Contractual ICT risk terms via enterprise onboarding
- - Operational resilience testing: customer-run; we document architecture/SLA
- - MSP maintains ICT register entry with honest gap disclosure

NIS2 (managed service supply chain)

- - Supply-chain transparency: subprocessors, architecture, Shipped/Gap tables
- - Security measures: signing policy, audit export, tenant isolation, MFA/RBAC
- - Incident notification: enterprise contract schedules
- - MSP/entity owns NIS2 conformity outcomes - not vendor badges

DPIA / ICT REGISTER BULLETS (pre-filled starters for MSPs)

Processing purpose: Signed PowerShell orchestration, script library, security audit Data categories: Admin identities, audit metadata, agent inventory, script content Controller (typical): MSP tenant; end-customer may be separate controller Processor (typical): Trustholm for platform operational data Subprocessors: See /trust/subprocessors; notify on changes per contract Security measures: Schema-per-tenant isolation, JWT tenant binding, MFA, signing Residency: Home region per contract schedule (EU option available) Gaps to disclose: WORM audit immutability backlog; native SIEM connector backlog Exit: Export audit/script data per contract; enterprise transition terms on request

Contact: security@trustholm.com for trust pack during regulated procurement.