TARA
INNOVA

GDPR Technical Measures Guide

How TARA INNOVA Supports GDPR Article 32 and Breach Notification Requirements

GDPR and Technical Security

The General Data Protection Regulation (EU 2016/679) requires controllers and processors to implement "appropriate technical and organisational measures" to ensure security of processing (Article 32). In practice, regulators and DPAs expect concrete, demonstrable technical controls — not policy documents alone. TARA INNOVA provides both the technical enforcement and the evidence to prove it.

Article 32 — Security of Processing

Article 32 requires measures appropriate to the risk, including:

Art. 32 Requirement	TARA INNOVA Coverage
32(1)(a) — Pseudonymisation and encryption	Quicksand enforces mTLS for all service communication. Session tokens with configurable TTL and IP binding. No plaintext sensitive data in transit.
32(1)(b) — Confidentiality, integrity, availability	Quicksand enforces access controls at the edge. Multi-deployment architecture ensures availability. Immutable audit logs ensure integrity of security records.
32(1)(c) — Restore availability and access after incident	Hybrid and multi-node deployment with no single point of failure. CRP documents recovery procedures and timelines.
32(1)(d) — Regular testing and evaluation	CRP provides continuous control effectiveness metrics. Trend analysis demonstrates ongoing security posture evaluation. Evidence of regular testing documented automatically.

Article 33 — Breach Notification

GDPR requires notification to the supervisory authority within 72 hours of becoming aware of a personal data breach. TARA INNOVA accelerates detection and documentation:

- **Real-time detection** — Quicksand identifies and blocks threats before data exfiltration occurs
- **Automatic incident documentation** — CRP generates breach reports with: nature of the breach, categories and number of data subjects, likely consequences, and measures taken
- **72-hour notification package** — Pre-formatted for DPA submission. Evidence chain from first indicator through containment
- **Article 34 support** — When breach notification to data subjects is required, CRP provides impact assessment and timeline documentation

Data Protection by Design (Article 25)

TARA INNOVA supports data protection by design and by default:

- **Data minimization** — Quicksand processes only traffic metadata for enforcement decisions. No personal data storage beyond security logs
- **EU data sovereignty** — Deploys entirely within your infrastructure. EU-headquartered. No third-country transfers
- **Access controls** — Role-based access across the platform. Least privilege enforcement. Audit trail on all administrative actions

- **Purpose limitation** — Security telemetry used only for enforcement and compliance evidence. No secondary processing

DPA and Regulator Engagement

When your Data Protection Authority investigates or audits, CRP provides immediate access to: technical security measure documentation, incident response evidence, control effectiveness metrics, and data processing activity records related to security operations. Evidence is pre-formatted for major EU DPAs including CNIL, BfDI, ICO, DPC, AEPD, Garante, and AP.