NIS2 supplier data sheet

OPEREX processes operational records at continuous-process, hazardous sites. If you fall under NIS2 (in Hungary, Act LXIX of 2024), Article 21(2)(d) makes you accountable for your suppliers' security as well. This sheet states WHAT OPEREX does in each measure group. We deliberately make no compliance claim — that judgement is yours and the authority's.

10/10	≤24 h	EU	117/117
Article 21(2) measures mapped	incident notification to you	primary data residency, on an encrypted volume	tenant tables isolated at database level

Notification of a security event

- ✓ We notify you within 24 hours of detecting a security event or personal data breach — by email, asking for acknowledgement.
- ✓ We notify even with partial information: we do not wait for the investigation to conclude, and we state when the next update is due.
- ✓ Why 24 hours: if you carry a reporting duty, your early warning is due within 24 hours — supplier notification has to serve that deadline.
- ✓ Reporting to the authority is your responsibility; we supply the factual detail needed for the investigation.

What we do not claim

- — We hold no ISO 27001 certificate. What exists: written policies, a data processing agreement listing the Article 32 measures, and measurable technical controls.
- — No external penetration test has been carried out yet — it is scheduled ahead of the first enterprise deployment.
- — There is no automatic failover. Protection comes from the 6-hourly, drill-proven backup.
- — Off-site backups are encrypted by the storage provider under its own keys; encryption under our own key is being introduced.
- — Security is handled by one person today, with a designated second emergency contact and a written continuity plan. For enterprise engagements, source-code escrow or an on-premise handover can be agreed.

This sheet records technical facts, not a legal assessment. For a detailed security overview or questionnaire support, please contact us.

ARTICLE 21(2) MEASURES AND OPEREX

a) Risk analysis, information security policies

A gap register with tracked identifiers, plus operational policies (incident response, access management, offboarding); a formal risk register and a regular review cycle are being established.

b) Incident handling

A written incident response plan with severity classes, an evidence-preservation step and a customer notification template. Detection: deep health checks, a log watcher and a push alert channel, plus external availability monitoring. Logs are copied off the server daily (90-day retention), so evidence survives a wiped local trail.

c) Business continuity, backup

Self-verifying off-site backups every 6 hours (SHA-256 read-back) with roughly a 6-hour recovery point, into an EU-jurisdiction store with a 90-day long-term tier. Restores are proven by drill, not assumed.

d) Supply chain security

A published sub-processor list in the legal documents, with 30 days' notice before engaging a new one. The software supply chain is built on locked dependencies, automated vulnerability tracking and a secret-leak gate. On exit, a complete data handover (every data table in machine-readable and spreadsheet form, with a file inventory and checksums), followed on request by a certified deletion.

e) Acquisition, development, vulnerability handling

Every change passes automated checks (tenant-isolation tests, a security scan, a secret gate), and a release cannot start until those are green. Vulnerability reports are received through an RFC 9116 channel.

f) Assessing effectiveness

Controls are guarded by machine gates that we deliberately break to measure — so it is proven that the gate actually catches. Independent code audits run regularly; an external penetration test is scheduled.

g) Cyber hygiene, training

Documented operating procedures and an access register; for the organisation using the product, the Help centre and Knowledge base provide usage guidance.

h) Cryptography, encryption

TLS on all traffic with HSTS; on the production server the database, the file store and local backups sit on an encrypted volume; passwords are hashed and two-factor secrets separately encrypted.

i) Access control, asset management

Invitation-only account creation, role-based access control, tenant isolation enforced at the database level and an append-only audit trail whose modification and deletion the database refuses for EVERY role. A maintained asset and access register, reviewed quarterly.

j) Multi-factor authentication

TOTP-based two-factor authentication is mandatory for platform administrator access and can be enforced per organisation for tenant administrators. On the operator side it is active on every external provider console.