



01 PLATFORM

Your operation. One clear system.

Opliora connects engineering, production, materials, quality and people around one traceable operational history - while the application and database remain inside the customer's infrastructure.

DESIGN	PLAN	BUILD	VERIFY
Controlled revision	Capacity and materials	Guided execution	Evidence and audit

At a glance

Manufacturing-first

Orders, drawings, BOMs, materials, routing, quality and workforce context.

Customer-controlled

PostgreSQL, network boundary, backups, retention and release timing remain under customer control.



02 ARCHITECTURE

Fits your architecture instead of replacing it.

A typical Opliora deployment uses a standalone application container behind the customer's reverse proxy, connected to a customer-managed PostgreSQL database and identity controls.

CUSTOMER NETWORK BOUNDARY

Reverse proxy / TLS / access policy

Opliora application container

Customer PostgreSQL database

Backups / monitoring / retention

Deployment

Docker-ready standalone build. Customer-managed reverse proxy and certificates.

Data

PostgreSQL under customer credentials. No shared Opliora customer database.

Identity

Role-based permissions, session controls, optional 2FA and scoped enterprise identity integration.

Operations

Customer-owned monitoring, backup, recovery, retention and production release schedule.



Security responsibilities remain explicit.

CONTROL	OPLIORA APPLICATION	CUSTOMER ENVIRONMENT
Access	Roles, permissions, sessions, optional 2FA	Identity source, network access, user lifecycle
Audit	Actor, time and affected record for critical actions	Review process, retention and escalation
Data	Application validation and controlled access paths	Database credentials, backups, restore testing
Release	Controlled application release and guidance	Test approval, maintenance window, rollback
Privacy	Protected sample data in public demo	Lawful basis, user notices, customer data governance

Integration surface

Common integration patterns include REST APIs, SMTP, barcode scanners, accounting exports, Active Directory or Microsoft Entra ID, and controlled spreadsheet imports. Exact interfaces are confirmed during discovery and validated in the customer environment.

 04 IMPLEMENTATION

Start focused. Prove value. Expand deliberately.

01	Map	Workflow, owners, source data and measurable baseline.
02	Install	Architecture, access, environments, monitoring and recovery.
03	Migrate	Clean, rehearse and validate selected operational records.
04	Pilot	Role-based training, live feedback and launch checks.
05	Launch	Controlled cutover and supported first production cycles.
06	Expand	Review evidence and select the next workflow or plant area.

Next step

Use the protected public demo to understand the interface, then schedule a technical discovery session to map Opliora to your network, data and first operational workflow.

Explore the live demo

www.nefab.uxui.ee

Technical conversation

hello@opliora.ee