ForezynPlan Financial Planning Platform

Security Overview

Enterprise-grade security for your most sensitive financial data.

SOC 2 Type II | ISO 27001 | GDPR | HIPAA | CSA STAR

Version 2.0 · April 2026 · Confidential

About ForezynPlan

ForezynPlan is an enterprise financial planning platform designed for modern finance teams. Our platform processes sensitive financial data on behalf of our customers, and we take our responsibility to protect that data seriously. This document is intended for security and procurement teams evaluating ForezynPlan as a vendor.

Security Principles

- Zero-trust architecture — every request is authenticated and authorised regardless of network origin
- Defence in depth — multiple independent control layers so no single failure compromises data
- Least privilege — users and services hold the minimum permissions required for their function
- Security by design — security requirements are built into every stage of the development lifecycle
- Transparency — we publish our security programme and engage openly with the research community

Compliance Summary

SOC 2 Type II	Annual audit covering Security, Availability & Confidentiality trust service criteria
ISO 27001	Certified ISMS; surveillance audits conducted bi-annually by accredited third party
GDPR	Full EU GDPR compliance; DPO appointed; Data Processing Agreements available
HIPAA	Business Associate Agreements (BAA) available for healthcare-covered entities
CSA STAR Level 1	Cloud Security Alliance self-assessment published and maintained
PCI DSS	Payments via PCI DSS Level 1 certified processors; card data never touches our systems

Infrastructure & Data Security

Cloud Hosting — Microsoft Azure

All ForezynPlan infrastructure is hosted on Microsoft Azure within ISO 27001 and SOC 2 Type II certified data centres. Data is stored in the EU (West Europe and North Europe regions) by default. Azure infrastructure is also compliant with GDPR, HIPAA, and FedRAMP.

- Virtual Networks (VNets) with strict ACLs; no public endpoints on production databases
- Azure DDoS Protection Standard on all public-facing services
- Azure Web Application Firewall (WAF) with OWASP Core Rule Set on all HTTP/S ingress
- Private Endpoints for all PaaS services (databases, storage, Key Vault)
- Infrastructure-as-code (Bicep/Terraform); no manual changes to production permitted

Encryption

Data at rest	AES-256-GCM encryption for all database and object storage
Data in transit	TLS 1.3 enforced for external; TLS 1.2 minimum for internal service-to-service
Key management	Azure Key Vault with HSM-backed key storage; customer-controlled key option
Database	Transparent Data Encryption (TDE) enabled on all relational databases
Backups	All backups encrypted with a separate key hierarchy; offsite copies encrypted at source

Data Residency & Backup

- Primary data stored in EU West Europe; hot standby in North Europe (secondary region)
- No data transferred outside the EEA without explicit customer consent and appropriate safeguards
- Configurable retention policies; default 7-year retention for financial records
- Automated point-in-time recovery (PITR) with 35-day recovery window
- Annual DR tests; documented RTO "d 4 hours, RPO "d 1 hour

Application & Operational Security

Application Security

- OWASP Top 10 mitigations embedded in the Secure Development Lifecycle (SDLC)
- SAST scanning on every pull request; critical findings block merge to main
- Software Composition Analysis (SCA) with automated CVE detection and patching SLA
- Annual penetration test by CREST-accredited third party; summary available under NDA
- Mandatory peer code review before any change reaches production
- Separate dev, staging, and production environments — no production data in lower environments

Authentication & Access Control

- SAML 2.0 / OIDC SSO integration for enterprise customers; enforced at tenant level
- Multi-factor authentication (MFA) mandatory for all users; TOTP and FIDO2 hardware keys supported
- Privileged Access Workstations (PAW) required for all production access by ForezynPlan engineers
- Just-in-time (JIT) access with time-limited elevation — no standing admin accounts in production
- All administrative actions written to a tamper-evident, immutable audit log

Monitoring & Incident Response

- Microsoft Sentinel SIEM with 24/7 automated alerting and security engineering on-call rotation
- User and Entity Behaviour Analytics (UEBA) for anomaly and insider-threat detection
- Immutable audit logs with 12-month hot retention; exportable in JSON and CSV
- Formal incident response plan with P0–P3 severity classification and documented runbooks
- P0 SLA: 15 minutes to page; 1 hour to mitigate; GDPR Art. 33 notification within 72 hours
- Post-incident reviews with root-cause analysis shared with affected customers

People Security & Contact

Employee Security

- Background checks and employment screening for all staff with production system access
- Mandatory security awareness training on joining and annually; quarterly phishing simulations
- All company devices enrolled in MDM with full-disk encryption and remote-wipe capability
- Strict joiners-movers-leavers process — access provisioned on day one, fully revoked on departure
- Quarterly access reviews for all personnel with elevated or production privileges
- Confidentiality agreements signed by all employees and contractors handling customer data

Responsible Disclosure

We welcome responsible disclosure from the security research community. If you discover a vulnerability in ForezynPlan, please report it to security@forezynplan.com with a description of the issue, steps to reproduce, and your assessment of the potential impact. We commit to a safe harbour — we will not pursue legal action against researchers acting in good faith. We aim to acknowledge all reports within 2 business days.

Contact & Document Requests

Security queries	security@forezynplan.com
Privacy / DPO	privacy@forezynplan.com
SOC 2 Type II report	Available under NDA — contact security@forezynplan.com
ISO 27001 certificate	Available on request — contact security@forezynplan.com
Penetration test summary	Available under NDA — contact security@forezynplan.com
Data Processing Agmt	Available at forezynplan.com/legal/dpa
Security page	forezynplan.com/security