Security, Hosting and Data Protection at DecisionBrain

Introduction

DecisionBrain is a leading partner in advanced **decision-support** software solutions, leveraging artificial intelligence (**AI**), mathematical **optimization** (Operations Research), and **predictive modeling** to address operational planning challenges — from supply chain and workforce planning to vehicle routing.

Information security is a strategic imperative at DecisionBrain and the foundation of client trust. Our **Information Security Management System** (ISMS), structured in accordance with **ISO/IEC 27001, 27017 and 27018** ensures the **Confidentiality, Integrity,** and **Availability** (CIA) of all digital assets entrusted to us.

Governance and Compliance

Executive Commitment

DecisionBrain's leadership has established a security policy aligned with ISO/IEC 27001, 27017 and 27018 with dedicated resources for continuous ISMS improvement and clearly defined cybersecurity responsibilities. The primary objective is to reduce any major risks (e.g. ransomware, data breaches) to zero.

Regulatory Compliance

In compliance with **GDPR**, DecisionBrain applies Privacy by Design from the earliest development stages. A dedicated Data Protection Officer (DPO) oversees personal data governance. We maintain a detailed record of processing activities and conduct Data Protection Impact Assessments (DPIAs) for all sensitive operations.

EUROCERTIFICATIONS ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

Certifications

Standard / Entity	Compliance / Certification
ISO/IEC 27001, 27017, 27018	Methodological framework of DecisionBrain's ISMS
GDPR	Full compliance; application of the SWIPO code of conduct
Scaleway (Primary CSP)	ISO 27001, HDS (Health Data Hosting), SecNumCloud (in progress)
DigitalOcean	SOC 2 Type II, SOC 3, CSA STAR Level 1
Microsoft Azure	ISO 27001, SOC 1/2/3, HIPAA, FedRAMP, IRAP
AWS	ISO 27001, SOC 1/2/3, PCI-DSS Level 1, HIPAA

Infrastructure and Hosting

Cloud-Native and Sovereign Architecture

Our platform is fully **infrastructure-agnostic**, supporting public cloud, private cloud, or air-gapped on-premise (disconnected cloud) deployments. We prioritize European-based providers — notably Scaleway — to ensure client data remains under European law (GDPR) and is not exposed to extraterritorial legislation. Hosting location is defined collaboratively with each client.

Dedicated, Non-Multi-Tenant Environments

Each client receives a **dedicated** Kubernetes cluster and Virtual Private Cloud (**VPC**), fully segregating development, UAT, and production environments. Container **hardening** via BellSoft base images reduces the operating system attack surface.

Security, Hosting and Data Protection at DecisionBrain

Identity and Access Management

Identity management is centralized via Keycloak using **OIDC**, **SAML 2.0**, **SSO**, and **LDAP**. Multi-factor authentication (MFA) is enforced for all employees' administrative and critical access.

Access rights follow a Role-Based Access Control (RBAC) model with the principle of least privilege and are immediately revoked upon employee offboarding.

Data Protection and Encryption

At Rest

AES-256 encryption is available for all storage volumes and databases (PostgreSQL, MongoDB). We leverage **Scaleway Block Storage** (SBS) encryption at the infrastructure level — transparent to Kubernetes and enabling online volume resizing without service interruption. Employee endpoints are encrypted via BitLocker or FileVault; removable media (USB) is prohibited.

In Transit

All communications are secured with **HTTPS** and **TLS 1.2/1.3** (Let's Encrypt certificates). Remote access and cluster administration use WireGuard or IPsec VPN tunnels.

Backup and Business Continuity

Backups are managed via BackupPC and cloud provider APIs, following a three-step workflow:



Kubernetes volume snapshots



Automated transfer to isolated S3 buckets



Immutable archiving via Scaleway's WORM (Write Once Read Many) Compliance mode

Our **Business Continuity Plan** (BCP) uses Terraform (Infrastructure as Code) for automated environment reconstruction. Critical function RTO is 24 hours, with monthly restoration tests. Crisis response runs from immediate mobilization (0–24h) through full service restoration (2–14 days).

Secure Development (DevSecOps)

Security is embedded throughout our CI/CD pipeline. SonarQube provides static analysis (SAST); Trivy and OWASP Dependency Check perform container and library scans for CVEs. Our practices align with the OWASP Top 10. Annual **penetration tests** are conducted by certified third parties as part of IBM's rigorous security review process. Four major versions of our platform **DB Gene** are released annually, each incorporating updated libraries and base images.

Monitoring and Incident Response

Real-time **observability** is provided by Prometheus, Grafana, and Loki. System and application logs are retained in S3 for a minimum of 90 days. Alerts are managed via AlertManager and Mattermost. In compliance with GDPR, any data breach posing a risk to individual rights is reported to the relevant supervisory authority within 72 hours, via encrypted communication channels and defined escalation protocols.

Conclusion

DecisionBrain combines technical excellence with organizational rigor to protect client data. Through isolated cloud-native architecture, ISO 27001, 27017 and 27018 alignment, and a DevSecOps culture, we deliver a decision platform that is high-performing, sovereign, and highly secure. Transparency and auditability remain the cornerstone of our mission.