digitalsamba

Security White Paper

Digital Samba Platform Security Whitepaper

Version: 1.0 Date: March 2026 Audience: CISOs, security architects, and compliance officers
Scope: Digital Samba Embedded and Digital Samba Free (current platform)

Table of Contents

1. Introduction

Digital Samba operates two video conferencing products built on a shared platform and infrastructure. Digital Samba Embedded is an API- and SDK-based platform that allows SaaS providers and enterprises to integrate white-label video conferencing into their own products. Digital Samba Free is a browser-based video conferencing tool for end users. Both products run on identical infrastructure with identical security controls.

This whitepaper describes the security architecture of the current Digital Samba platform. It covers infrastructure, cryptography, access control, application security, and organisational controls.

The platform processes the following data categories during normal operation: real-time audio and video streams, screen sharing content, chat messages, shared files, participant display names, session metadata (join/leave times and participant counts), and API credentials. Real-time media streams are transient; chat messages, shared files, and session recordings are retained on behalf of customers.

> To request additional documentation, including a Data Processing Agreement (DPA) or supplementary compliance materials, contact **security@digitalsamba.com**.

2. Architecture Overview

The Digital Samba platform is composed of several distinct service tiers, each with a defined role and network boundary.

The web server serves the application front end over HTTPS and handles session initialisation. The signalling server manages WebRTC session negotiation and participant coordination over encrypted WebSocket connections. The media server, implemented as a Selective Forwarding Unit (SFU), receives individual participant media streams and routes them to other participants without mixing. The TURN (Traversal Using Relays around NAT) server provides media relay for participants behind restrictive firewalls or NAT. The recording server handles session recording where enabled; it is isolated from the primary media path and accessible only via internal IP allowlisting. The API layer provides programmatic access to platform functions for Embedded integrations and is authenticated via scoped API keys.

Production infrastructure runs across Leaseweb Netherlands (Amsterdam) and Scaleway (France, Netherlands, and Poland). Disaster recovery and backup infrastructure operates in a separate EU data centre (Leaseweb Deutschland GmbH, Frankfurt, Germany). During periods of peak demand, the platform scales to Scaleway as the primary overflow provider; Exoscale / Akenes SA (Switzerland) serves as secondary overflow capacity. The encryption controls described in Section 3 (TLS configuration, DTLS-SRTP for media transport, and encryption at rest) apply uniformly across all infrastructure providers. All providers process encrypted media streams in transit; they do not have access to E2EE session content (see Section 3.3).

DNS is managed via Amazon Web Services (AWS) Route 53. Route 53 handles name resolution only and processes no application or session data. Data processing terms covering this relationship under GDPR Article 28 are in place through the AWS Data Processing Addendum; the transfer mechanism is the EU-US Data Privacy Framework combined with Standard Contractual Clauses (SCCs). AWS processes only resolver IP addresses; no application-level personal data is involved.

Production, staging, and development environments are separated at the network level. Production data is not used in non-production environments unless anonymised.

The platform supports on-premises deployment for customers who require full control over infrastructure. In an on-premises deployment, the customer operates all platform components on their own infrastructure. Digital Samba provides the software and integration support; the customer is responsible for the security of the deployment environment.

3. Data Security

The encryption controls described in this section implement Digital Samba's obligations under GDPR Article 32, which requires controllers and processors to implement appropriate technical measures to ensure a level of security appropriate to the risk.

3.1. Encryption in Transit

All external interfaces use TLS (Transport Layer Security) 1.3 where supported by connecting clients, with TLS 1.2 as the minimum supported version. TLS 1.0 and TLS 1.1 are disabled on all production services. HTTP Strict Transport Security (HSTS) is enforced on all web-facing services, preventing protocol downgrade attacks.

TLS certificates are renewed automatically on a 90-day cycle. All certificates use RSA 2048-bit or ECDSA P-256 as a minimum. The following table describes the protocol and port used for each public-facing interface.

Interface	Protocol	Port
User → Web Server	HTTPS (TLS)	443
User → Signalling Server	WSS (TLS WebSocket)	443
User → Media Server API	HTTPS (TLS)	443
User → Media Server (media streams)	DTLS-SRTP (UDP)	1024–65535
User → TURN Server (negotiation)	HTTPS (TLS)	443
User → TURN Server (media relay, UDP path)	DTLS-SRTP (UDP)	1024–65535
User → TURN Server (media relay, TCP fallback)	HTTPS (TLS)	443

Port 80 is exposed on the web server solely to redirect HTTP requests to HTTPS. All requests on other ports are dropped at the firewall. The DTLS handshake establishes the SRTP and SRTCP cryptographic contexts for media.

Internal services are not exposed to the public internet. Access is restricted to authorised systems only.

3.2. Encryption at Rest

Data stored on Digital Samba infrastructure is encrypted at rest using AES-256-GCM (Advanced Encryption Standard, 256-bit key, Galois/Counter Mode). This applies to database storage, session

recordings, and all backup data. This control implements ISO 27001:2022 Annex A control A.8.24 (Use of cryptography).

Backups are encrypted at rest with AES-256-GCM and transmitted to the off-site backup location over SSH, which provides encryption in transit for backup data. The backup location (Leaseweb Deutschland, Frankfurt) is a separate physical site from the production environment (Leaseweb Netherlands, Amsterdam). This geographic separation ensures that a data centre-level event affecting production does not simultaneously affect backup availability.

Key management for data-at-rest encryption follows a defined cryptography policy. AES-256-GCM is the required algorithm. Encryption key rotation procedures are defined in the policy. Customer-managed key options are not currently available for cloud-hosted deployments; on-premises customers control their own key management infrastructure.

3.3. End-to-End Encryption

Transport encryption (TLS and DTLS-SRTP) protects data in transit between participants and the platform. Transport encryption operates hop by hop: the media server decrypts and re-encrypts streams as it routes them, which means the server has access to plaintext media in the standard configuration.

Digital Samba supports optional end-to-end encryption (E2EE) at the application layer to address this. When E2EE is enabled, media is encrypted on the participant's device before it leaves the browser. The Digital Samba infrastructure (signalling servers, media servers, and hosting providers) receives and forwards only ciphertext. It has no access to decryption keys and cannot inspect session content. This control implements ISO 27001:2022 Annex A controls A.8.24 (Use of cryptography) and A.8.26 (Application security requirements).

Data protected by E2EE includes: audio streams, video streams, screen sharing content, chat messages, participant display names, and whiteboard data.

Encryption implementation. Each participant generates encryption key material locally within their browser using the Web Crypto API. For real-time media, the platform uses AES-256-GCM, which provides both confidentiality and authenticated integrity. Encryption is applied to media packets at the application layer before the WebRTC transport stack transmits them. The result is two complementary layers of protection: application-layer encryption ensuring that only session participants can decrypt content, and transport-layer encryption (DTLS-SRTP) protecting packets during network transmission.

Key exchange. Participants establish a shared encryption context through a cryptographic key agreement protocol. Each participant generates private key material locally; private keys do not leave the device. Only the information necessary to establish a shared secret is exchanged through the signalling server. The signalling infrastructure does not receive or store private keys or session decryption keys.

Key rotation. The platform implements dynamic key rotation throughout the session lifetime. When a participant leaves, encryption keys are refreshed so that the departed participant cannot decrypt future communication (forward secrecy). When a new participant joins, previously transmitted content cannot be decrypted retroactively (backward secrecy). These two properties together ensure that encryption keys are valid only for the intended participants and only for the duration of their participation.

Media server role. In an E2EE session, the SFU receives encrypted packets and forwards them to the appropriate participants based on routing metadata. It does not have access to decryption

keys and cannot inspect, transcode, or analyse media content. This is an architectural constraint, not a policy constraint.

Security verification. The platform provides an in-session security code derived from the cryptographic keys of all current participants. Participants can compare this code through an out-of-band channel (for example, by reading it aloud) to verify that all participants share the same encryption context. A mismatch indicates a potential man-in-the-middle or signalling manipulation attack.

Feature limitations. Because the server cannot access decrypted content in E2EE mode, server-side recording and server-side media analysis (e.g. transcription) are not available in E2EE sessions. E2EE is intended for scenarios that prioritise maximum confidentiality over server-side capabilities.

4. Access Control

4.1. Internal Access Controls

Multi-factor authentication (MFA) is required on all systems that support it, including all core business and production systems. Authenticator apps are the standard MFA method; SMS-based codes are permitted only where no alternative exists. Passwords for critical systems must be at least 16 characters, generated by a password manager, and unique per system. Password reuse is prohibited. These controls implement ISO 27001:2022 Annex A controls A.5.15 (Access control), A.5.16 (Identity management), and A.5.18 (Access rights).

SSH access to production servers requires a VPN connection. Key-based authentication is required; password-based SSH authentication is disabled. SSH keys use Ed25519 or RSA 4096-bit as a minimum. Direct pushes to production infrastructure require explicit authorisation from an appropriate approver.

Access requests are submitted through an auditable channel with approval records retained. Access to critical systems is reviewed quarterly; all other access is reviewed annually. When a team member departs the organisation, access to critical systems is revoked immediately; access to non-critical systems is revoked within 7 days. Separation of duties applies to financial transactions, production code deployment, and user provisioning. The default access policy is deny-all; access is granted only through an explicit approval process.

4.2. Product Authentication and Authorisation

The Digital Samba Embedded API uses scoped API keys for authentication. Keys are issued per integration and can be restricted to specific operations. Customers manage their own API key lifecycle through the developer dashboard.

The platform supports role-based access control (RBAC) within sessions. Roles include host, moderator, and participant, each with a defined set of permissions covering media control, participant management, and content sharing. Role assignments are enforced server-side; clients cannot escalate their own permissions.

Enterprise customers requiring SSO (Single Sign-On) integration for their administration portal should contact Digital Samba to discuss available authentication options.

Session tokens are scoped to the specific session and participant. Token validity and expiry parameters are configurable by the customer integration.

5. Application Security

5.1. Secure Development Lifecycle

All code changes require a pull request in the version control system. Direct pushes to the main and production branches are prohibited by branch protection rules, as are force pushes. Production deployments are controlled through a tagging process. These controls implement ISO 27001:2022 Annex A controls A.8.25 through A.8.33 (secure development lifecycle).

The following controls are enforced at the code level: parameterised queries are required for all database access (constructing SQL from user input is prohibited); input validation and output encoding are required to prevent injection and cross-site scripting (XSS) vulnerabilities; secrets (API keys, credentials, and cryptographic material) must never be committed to source code repositories. Development environments use non-production credentials. Production data is not used in development or testing unless anonymised.

Dependency management follows a defined process: lock files are required for all package managers; security patches to dependencies are prioritised over feature work; and unused dependencies are removed. Developers review the security posture of new dependencies before adding them to a project.

Emergency changes to production infrastructure are subject to a defined exception process with mandatory post-change review.

5.2. Penetration Testing

Digital Samba conducts regular penetration testing of the platform.

5.3. Vulnerability Reporting

Security researchers and customers who identify a potential vulnerability in the Digital Samba platform should report it to security@digitalsamba.com. Reports are triaged and acknowledged, and Digital Samba coordinates with reporters through resolution.

5.4. Dependency and Vulnerability Scanning

Static analysis and dependency vulnerability scanning are integrated into the build pipeline. Security patches are prioritised in the development backlog. Dependency vulnerabilities are tracked and remediated according to severity, with critical vulnerabilities prioritised for immediate resolution.

6. Infrastructure Security

6.1. Physical Security and Data Centre Controls

Production infrastructure is housed at Leaseweb Netherlands B.V. (Amsterdam) and Scaleway SAS (multiple EU countries). Both providers operate Tier III data centres with 24/7 physical security, biometric access controls, CCTV, and redundant power and cooling.

The following certifications are held by Leaseweb Netherlands.

Certification	Scope and Notes
ISO 27001:2022	Information security management system; covers the full Leaseweb Netherlands operation
SOC 1 Type II	Controls over financial reporting; covers Leaseweb systems as they affect customer financial processes. Note: SOC 1 addresses financial reporting controls, not information security controls in the SOC 2 sense
PCI DSS	Physical security controls only (requirements 9 and 12). Digital Samba does not process payment card data through Leaseweb systems
CISPE	Cloud Infrastructure Services Providers in Europe. An EDPB-approved code of conduct under GDPR Article 40, verifying GDPR-compliant IaaS operation and data processing within the EU/EEA

Leaseweb Netherlands also holds an EY third-party alignment statement for NEN 7510:2017 (the Dutch healthcare information security standard). This is an alignment assessment, not a formal certification. Healthcare customers evaluating the platform should factor this distinction into their assessment.

The following certifications are held by Scaleway SAS.

Certification	Scope and Notes
ISO 27001:2022	IInformation security management system
SOC 1 Type II	Hébergeur de Données de Santé (Health Data Hosting); certified under French law for hosting health data

Scaleway is currently pursuing SecNumCloud qualification, ANSSI's sovereign cloud security standard. This qualification is in progress and has not yet been granted.

The disaster recovery and backup site (Leaseweb Deutschland GmbH, Frankfurt) holds equivalent certifications to Leaseweb Netherlands: ISO 27001:2022, SOC 1 Type II, PCI DSS (physical), and CISPE.

Leaseweb's infrastructure-layer Security Operations Centre (SOC) provides continuous security monitoring at the hosting level, including SIEM (Security Information and Event Management) and intrusion detection at the network perimeter.

6.2. Network Security and Segmentation

Production, staging, and development environments are separated at the network level. Production systems are not reachable from development or staging environments.

DDoS (Distributed Denial of Service) protection is provided at the network layer by Leaseweb's globally distributed scrubbing infrastructure, which detects and mitigates volumetric and protocol-based attacks (Layers 3 and 4) affecting the production environment.

6.3. Host Hardening and Patch Management

Production servers follow an internal hardening baseline that disables unnecessary services and restricts network exposure. Critical security patches are prioritised for prompt application. Detailed information about hardening standards and patch management cadence is available on request to enterprise customers undergoing vendor diligence; contact security@digitalsamba.com.

6.4. Endpoint Security

All team members and contractors who access company systems must have full-disk encryption enabled on their devices. Compliance with this requirement is verified as part of the onboarding process.

7. Availability and Resilience

7.1. Infrastructure Redundancy

Production workloads run across Leaseweb Netherlands (Amsterdam) and Scaleway (multiple EU countries, ISO 27001:2022 and HDS certified). During peak demand, Scaleway serves as the primary overflow provider; Exoscale / Akenes SA (Switzerland, ISO 27001:2022, ISO 27017, ISO 27018, ISO 22301:2019, SOC 2 Type II, PCI DSS v4.0, BSI C5, CSA STAR, and HDS certified) provides secondary overflow capacity. This multi-provider architecture ensures that platform capacity is not constrained to a single data centre and is not entirely dependent on a single provider's availability.

7.2. Backup and Recovery

Backups run daily, mirroring production data from Leaseweb Netherlands (Amsterdam) to Leaseweb Deutschland (Frankfurt). Filesystem snapshots are created after each backup operation. Database backups are produced in parallel with file-level backups, providing two independent

recovery paths: file-level restoration and logical database restoration. Integrity is verified using checksums on each operation. This control implements ISO 27001:2022 Annex A control A.8.13 (Information backup).

Backups are retained for a rolling 90-day window. The backup site is in a separate country from production (Germany versus the Netherlands), satisfying geographic separation requirements for disaster recovery. Backup restoration is tested quarterly; restoration procedures are documented and test results are recorded.

Backup data is encrypted at rest using AES-256-GCM and transmitted over SSH.

Daily backups establish a nominal Recovery Point Objective (RPO) of 24 hours. Formal RPO and Recovery Time Objective (RTO) commitments are defined in the service agreement. Customers requiring specific availability guarantees should review these commitments with Digital Samba during the contracting process.

7.3. Service Availability

Platform availability commitments are defined in the service agreement. Customers evaluating Digital Samba for business-critical deployments should request the current service level terms from their account representative or contact security@digitalsamba.com.

8. Compliance and Certifications

8.1. Digital Samba's Own Compliance Posture

Digital Samba is building an Information Security Management System (ISMS) structured around ISO 27001:2022 as a reference framework. The ISMS policy framework covers security policy, risk management, access control, cryptography, operations security, incident management, and supplier management. Digital Samba does not currently hold ISO 27001 certification from an accredited certification body and has not completed a SOC 2 Type II audit.

A Statement of Applicability (SoA) mapping Digital Samba's controls to ISO 27001:2022 Annex A is available on request to enterprise customers conducting vendor diligence.

> Customers who require a Data Processing Agreement or supplementary security documentation should contact **security@digitalsamba.com**.

8.2. GDPR Compliance

Digital Samba processes personal data as a data processor on behalf of customers who use the platform for their own video conferencing sessions. Digital Samba also processes personal data as a data controller for account management and platform operation. Where a customer acts as a processor on behalf of its own controller, Digital Samba acts as sub-processor within the meaning of GDPR Article 28(4); the DPA provides for this scenario.

A Data Protection Officer (DPO) has been designated in accordance with GDPR Article 37. Digital Samba is registered in Spain; the competent supervisory authority is the Agencia Española de Protección de Datos (AEPD). Records of Processing Activities (ROPA) are maintained as required

by GDPR Article 30. Data processing terms compliant with GDPR Article 28 are in place with all infrastructure providers, whether through dedicated DPAs or provider terms of service. Data Protection Impact Assessments (DPIAs) are conducted for high-risk processing activities. The lawful basis for each processing activity is documented in the ROPA.

Core platform data (production and backup) remains within the European Union. Production infrastructure is in the Netherlands; backup infrastructure is in Germany. DNS resolution via AWS Route 53 involves no transfer of application or session data; it is limited to domain name lookups and is covered by DPF and SCCs (see Section 2).

8.3. Applicable Frameworks

The platform architecture and hosting choices are designed to support customer compliance with the following frameworks, where applicable to the customer's own regulatory environment.

NIS2 (Network and Information Systems Directive 2): The ISMS, incident response procedures, and supplier management programme are structured to support NIS2 obligations. NIS2 applicability depends on the customer's own regulatory classification; Digital Samba's platform supports customers' NIS2 compliance efforts. Customers who need to assess Digital Samba's controls against specific NIS2 requirements should contact security@digitalsamba.com.

NEN 7510 / Healthcare: Leaseweb Netherlands holds an EY third-party alignment statement for NEN 7510 (not a formal certification; see Section 6.1). Scaleway holds HDS (Health Data Hosting) certification under French law. Healthcare customers requiring data processed within HDS-certified infrastructure should contact Digital Samba to discuss deployment options.

HIPAA (Health Insurance Portability and Accountability Act): Digital Samba's primary EU infrastructure is not operated under a HIPAA Business Associate Agreement (BAA). Customers subject to HIPAA have two options: Digital Samba can provide US-based infrastructure hosted with a HIPAA-eligible provider, or customers can choose the on-premises deployment option, which provides full control over the infrastructure environment and allows the customer to execute a BAA with their own infrastructure provider. Contact Digital Samba to discuss HIPAA deployment requirements.

9. Data Processing, Retention, and Privacy

9.1. Data Categories

The platform processes the following categories of data.

Real-time media streams (transient): Audio, video, and screen sharing streams during active sessions. When E2EE is not enabled, this data passes through the media server in plaintext; the platform processes it only to route it to participants and does not retain it after the session ends.

Persistent session content: Chat messages, shared files, and other session artifacts are retained after the session ends and remain accessible to the customer through the API and dashboard.

Session recordings: Where recording is enabled by the session host, the platform generates an MP4 recording capturing audio, video, and screen sharing. Recordings are stored on platform infrastructure, encrypted at rest (AES-256-GCM), and accessible only through authenticated API calls or the customer dashboard.

Participant metadata: Join and leave timestamps, participant counts, session duration, and connection quality metrics. This data is used for platform operation and analytics.

Account and API credentials: Customer account information, API keys, and associated metadata for Digital Samba Embedded customers.

9.2. Retention Periods

Real-time media streams (audio, video, screen sharing) are not retained after the session ends. Persistent session content such as chat messages and shared files is retained until deleted by the customer or upon contract termination. Recordings are retained according to the retention settings configured by the customer; the platform does not impose a minimum retention period on customer recordings.

System logs and security event records are retained for defined periods (see Section 12 for details). Backup snapshots are retained for a rolling 90-day window. After the 90-day window has elapsed, previously deleted data is no longer present in any backup snapshot.

Incident records are retained for 3 years. Personal data breach records are retained for 6 years, in accordance with the internal retention schedule, which aligns with applicable limitation periods and GDPR Article 5(2) accountability obligations.

9.3. Data Deletion and Subject Rights

Upon contract termination, customer data is deleted according to the terms of the service agreement and DPA. Customers can request deletion of specific data at any time. Data subject requests (access, rectification, erasure, portability, and restriction) are acknowledged and fulfilled within one month, as required by GDPR Article 12.

9.4. Data Residency

Production data is hosted in the Netherlands and across multiple EU countries via Scaleway. All backup data is stored in Germany. No application or session data is stored outside the EU or EEA. Customers who require data residency guarantees for a specific EU member state should discuss this with Digital Samba; the on-premises deployment option provides the strongest residency guarantees.

9.5. Sub-processors

Digital Samba's infrastructure sub-processors are: Leaseweb Netherlands B.V. (production), Scaleway SAS (production and primary overflow), Leaseweb Deutschland GmbH (backup and DR), and Exoscale / Akenes SA (secondary overflow). A full sub-processor list, including non-infrastructure SaaS suppliers that may process personal data on behalf of customers, is available in the DPA.

10. Incident Response

Digital Samba classifies security incidents into four severity levels. Severity 1 (Critical) incidents require CISO notification within 1 hour and initiate immediate response procedures. Lower severity

levels have progressively longer notification windows; all incidents require a documented response. These controls implement ISO 27001:2022 Annex A controls A.5.24 through A.5.28 (Information security incident management).

Incidents are categorised by type: security incident, personal data breach, service disruption, near-miss, and vulnerability disclosure. Personal data breaches follow a separate, accelerated process: the Data Protection Officer is notified immediately upon identification, and the AEPD (as the competent supervisory authority) is notified within 72 hours as required by GDPR Article 33. For breaches posing a high risk to the rights and freedoms of data subjects, affected individuals are notified without undue delay in accordance with GDPR Article 34.

Post-incident reviews are conducted after all Severity 1 and Severity 2 incidents. Reviews examine root cause, response effectiveness, and any changes to controls or procedures required.

Customers affected by security incidents or data breaches are notified through the communication channels and within the timelines specified in the DPA. The DPA defines specific notification obligations and the information to be provided. Customers who have not yet executed a DPA should request one to review the notification commitments.

Incident records are retained for 3 years. Personal data breach records are retained for 6 years.

11. Personnel Security

Digital Samba's core team consists of contractors and external collaborators rather than direct employees. The controls described in this section apply to all team members and contractors with access to company systems or customer data.

All new team members complete security awareness training before being granted access to production systems. Security training is conducted annually for all staff.

Background checks are conducted for team members and contractors in accordance with applicable law and the sensitivity of the role. All team members sign confidentiality agreements and an acceptable use policy on engagement.

Access is provisioned using the principle of least privilege and requires explicit approval through the documented access request process. When a team member departs the organisation, critical system access is revoked immediately on the last working day. Non-critical system access is revoked within 7 days.

12. Audit and Logging

Platform systems record authentication events, authorisation decisions, administrative actions, API access, and security events. Security event logs include system administrator activity. Logs are reviewed regularly as part of operational security procedures. These controls implement ISO 27001:2022 Annex A controls A.8.15 (Logging) and A.8.16 (Monitoring activities).

Leaseweb Netherlands' data centre infrastructure includes a Security Operations Centre (SOC) that performs continuous SIEM monitoring and intrusion detection at the infrastructure layer.

Logs are stored separately from the systems that generate them. Specific log retention periods and tamper protection mechanisms for application-level security logs are defined in internal operational procedures; details are available on request to enterprise customers conducting vendor diligence.

13. Third-Party and Vendor Management

Digital Samba maintains a supplier register covering all third-party providers with access to company systems or customer data. Each supplier is assessed during onboarding for security certifications, data residency commitments, and GDPR compliance. Suppliers with access to personal data must have data processing terms compliant with GDPR Article 28 in place before access is granted, whether through a dedicated DPA or the supplier's terms of service. These controls implement ISO 27001:2022 Annex A controls A.5.19 through A.5.22 (Supplier relationships).

Infrastructure suppliers are assessed in depth. The due diligence process for each hosting provider covers applicable certifications, data centre physical security controls, incident response and notification obligations, sub-processing and data transfer restrictions, and GDPR Article 28 compliance.

Key infrastructure supplier certifications are summarised below.

Provider	Role	Key Certifications
Leaseweb Netherlands B.V.	Production (Amsterdam)	ISO 27001:2022, SOC 1 Type II, PCI DSS (physical), CISPE, NEN 7510 (EY alignment statement, not a certification)
Leaseweb Deutschland GmbH	Backup and DR (Frankfurt)	ISO 27001:2022, SOC 1 Type II, PCI DSS (physical), CISPE
Scaleway SAS	Production and primary overflow (EU)	ISO 27001:2022, HDS
Exoscale / Akenes SA	Secondary overflow (Switzerland)	ISO 27001:2022, ISO 27017, ISO 27018, ISO 22301:2019, SOC 2 Type II, PCI DSS v4.0, BSI C5, CSA STAR, HDS
Amazon Web Services	Route 53 DNS (name resolution only)	ISO 27001, SOC 1/2/3, PCI DSS, FedRAMP, HIPAA

Supplier security posture is reviewed annually or upon significant change to the supplier relationship.

14. Key Commitments Summary

The following table consolidates key security and operational commitments described in this whitepaper for quick reference.

Domain	Commitment	Reference
Encryption in transit	TLS 1.3 standard, TLS 1.2 minimum; TLS 1.0/1.1 disabled	Section 3.1
Encryption at rest	AES-256-GCM for all stored data and backups	Section 3.2

Domain	Commitment	Reference
End-to-end encryption	Optional application-layer E2EE with AES-256-GCM; forward and backward secrecy	Section 3.3
MFA	Required on all systems; authenticator apps as standard	Section 4.1
SSH access	VPN + key-based authentication; Ed25519 or RSA 4096-bit minimum	Section 4.1
Access reviews	Quarterly for critical systems; annually for all others	Section 4.1
Access revocation	Immediate for critical systems; within 7 days for standard	Section 4.1
Code changes	Pull requests required; branch protection enforced; tag-based deployment	Section 5.1
Backup frequency	Daily with filesystem snapshots; database dumps in parallel	Section 7.2
Backup retention	90-day rolling window	Section 7.2
Backup restoration testing	Quarterly	Section 7.2
Backup encryption	AES-256-GCM at rest; encrypted in transit via SSH	Section 7.2
Geographic separation	Production in NL; backup/DR in DE	Section 7.2
Incident response (Severity 1)	CISO notification within 1 hour	Section 10
Breach notification (supervisory authority)	Within 72 hours (GDPR Article 33)	Section 10
Data subject requests	Fulfilled within one month (GDPR Article 12)	Section 9.3
Data residency	All application data within the EU	Section 9.4
Supplier reviews	Annual or upon significant change	Section 13
Availability SLA, RTO, RPO	Defined in service agreement; contact Digital Samba	Section 7.2, 7.3

This document reflects the security posture of the Digital Samba platform as of the date indicated. Digital Samba is actively developing its ISMS and compliance programme; certification milestones will be reflected in future revisions of this document.