sea.dev SECURITY · WHITEPAPER

Security whitepaper

Deployment, data protection, governance and compliance at Sea.dev.

Last updated: July 2026

Sea.dev provides AI for lending teams, automating document processing, financial spreading and underwriting support. Our customers are regulated lenders and financial institutions. This paper sets out how we deploy, protect and govern their data.

1. Our role

Sea.dev acts as a **processor** of the data you submit; you remain the **controller**. The platform runs inside your environment, lending decisions stay with your team, and we work to remove any dependency that moves data outside it.

Three principles apply to every deployment: on-premises with no data egress, a route off commercial models, and human review of every output.

2. Deployment models

We offer three deployment models:

- **Cloud.** Compute, storage and processing in our AWS environment.
- **Customer-managed cloud.** A single-tenant deployment in your own Azure, GCP or AWS account — isolated, encrypted, and penetration-tested before it goes live.
- **On-premises.** A full on-premises deployment with no data egress, for the most sensitive environments.

A typical engagement begins with a single-tenant environment in your cloud account, which we then help you move fully in-house; alternatively, we deploy on-premises from the start. You own the infrastructure, the keys and the audit trail throughout.

3. Data egress

On-premises and self-hosted deployments run with no data egress. In cloud pilots, inference currently runs on OpenAI, which does not train on data sent through its API. We treat this as a dependency to remove:

- Begin on OpenAI to reach production quickly.

- Tune the workflow on your historical data and validate it against an agreed accuracy threshold.
- Migrate to open models hosted inside your environment, so the whole pipeline, inference included, runs with no egress.

4. Data protection and encryption

- **Encryption in transit:** TLS 1.3.
- **Encryption at rest:** AES-256.
- **Key management:** AWS KMS, or your own KMS in customer-managed and on-premises deployments.
- **Isolation:** storage is encrypted and separated per organisation.
- **Training:** your data is never used to train models.
- **Residency:** processing is confined to the deployment you choose.

5. Identity and access

- Single sign-on with Microsoft Azure and SAML 2.0.
- Multi-factor authentication.
- Role-based access control and managed API keys.
- Audit logs of user and system activity, exportable to your own monitoring.

6. Governance

Sea.dev does not make lending decisions. It reads submitted documents, extracts the key information, checks it across sources to flag inconsistencies, and presents the results and any exceptions to an analyst to review and accept. Every correction and rejection is logged.

RNHB, a specialist real-estate lender in the Netherlands, embedded Sea.dev in its origination workflow. The system was tuned on RNHB's historical data and met an agreed accuracy threshold before go-live; in production, every analyst correction is logged and the credit decision stays with an RNHB employee.

7. Compliance and legal

- **GDPR & UK GDPR.** We process personal data as a processor on your documented instructions.

- **International transfers.** Where required, transfers rely on the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914) and the UK International Data Transfer Addendum.
- **State privacy laws.** Our Data Processing Agreement covers US state laws including the CCPA and the Colorado, Virginia, Connecticut and Utah privacy acts, where applicable.
- **Data Processing Agreement.** A DPA is available, covering the security measures, sub-processing terms and transfer mechanisms set out here.
- **Personal data breach.** We notify you without undue delay once we confirm a breach affecting your data, with the information you need to meet your own obligations.
- **Audit rights.** The DPA provides for audits, including on-premises inspection, and accepts SOC 2 Type 2, ISO or NIST reports from qualified third-party auditors.
- **Return and deletion.** On termination we return or securely delete your data in line with your instructions and our backup deletion routines.
- **Governing entity.** seadotdev Limited, registered in England & Wales; governing law of England and Wales.

8. Testing and assurance

- **Penetration testing.** An independent third party tests our cloud and container security every 3–6 months. The most recent assessment was completed in Q2 2026; a certificate is available under NDA.
- **SOC 2.** A SOC 2 Type I audit is underway, with Type II to follow.
- **Monitoring.** Our security posture, policies and current sub-processor list are maintained on our Vanta Trust Center, with reports available under NDA.

9. Sub-processors

We keep a current list of sub-processors, with their function and location, on our Trust Center, and give advance notice of changes. Each sub-processor is bound by terms at least equivalent to those we commit to you.

10. Contact

For a security review, questionnaire, or copies of reports under NDA, contact security@sea.dev. Live status and documentation are on our Vanta Trust Center.
