SettlDay

SETTLEMENT READINESS PLATFORM

GET IT DONE

Vendor Due Diligence Pack

Version dc151e3
Generated 2026-04-14

SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

settlday.com

Contents

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

1. GDPR Compliance Summary

Document ID	TC-GDPR-001
Classification	Public – Trust Center

1.1 Scope

This document summarises the GDPR compliance posture of amalics GmbH (trading as SettlDay) under the General Data Protection Regulation (EU 2016/679). It covers all personal data processing activities across the SettlDay platform, a B2B SaaS application that helps mid-market financial firms prepare for T+1 settlement transition.

Data Controller: amalics GmbH, Simrockstr. 23, 80997 Munchen, Germany Registered at Amtsgericht Munchen, HRB 264611

1.2 Personal Data Categories

SettlDay processes the following categories of personal data:

Category	Description	Sensitivity
Professional identity	First name, last name, email address	Low – business contact information
Professional role	Company name, job title	Low – business context
Firm profile	Firm type, firm size, region of operation	Low – quasi-identifiers, not directly identifying
Account credentials	Managed by a self-hosted identity provider on SettlDay's own EU infrastructure; not stored in the application database	Medium
Assessment scores	Numerical maturity scores per assessment category	Low – linked to anonymous sessions
Payment data	Card details handled entirely by Stripe; payment data never touches SettlDay servers	High (managed by Stripe under PCI DSS Level 1)

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

SettlDay does not process special category data (Art. 9) – no health, biometric, racial, political, or religious data is collected.

1.3 Legal Bases for Processing

1.3.1 Consent (Art. 6(1)(a))

Applies to report requests and waitlist registrations. Explicit consent is obtained via checkboxes before any personal data collection, with separate consent for report delivery, advisory follow-up, and waitlist registration. Consent timestamps are recorded. Users may withdraw consent at any time through self-service endpoints or by contacting privacy@settlday.com.

1.3.2 Performance of Contract (Art. 6(1)(b))

Applies to registered user accounts and organisations. User accounts are created as part of the B2B service agreement; processing is necessary to provide the contracted platform services.

1.3.3 Legal Obligation (Art. 6(1)(c))

Applies to data subject access request (DSAR) records. DSAR records are maintained to demonstrate compliance with data subject rights under Art. 15-22.

1.3.4 Legitimate Interest (Art. 6(1)(f))

Applies to anonymous assessment sessions capturing firm type, firm size, and region. This data tailors assessment questions to the firm's regulatory context. Sessions are anonymous by default – no personal data is collected unless the user explicitly requests a report. The benefit of personalised assessment outweighs the minimal privacy impact of professional firm-level data.

1.4 Data Retention Periods

Data Category	Retention Period	Enforcement
Report requests (PII)	2 years from creation	Automated daily enforcement – PII is anonymised on expiry
Waitlist entries (PII)	1 year from creation	Automated daily enforcement – PII is anonymised on expiry
Assessment sessions	2 years from completion	No PII; retained for analytics
Deleted user accounts	90-day grace period after deletion	Automated hard-purge after grace period

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Data Category	Retention Period	Enforcement
DSAR audit records	3 years from creation	Automated hard-purge after retention period

Retention enforcement is fully automated. A scheduled task runs daily and anonymises or purges records that have exceeded their retention period. No manual intervention is required.

1.5 Data Subject Rights

SettlDay implements all data subject rights under GDPR Art. 15-22 through a combination of self-service endpoints and email-verified request flows:

Right	GDPR Article	Implementation
Right of access	Art. 15	Self-service endpoint with email verification; returns all personal data in structured format
Right to rectification	Art. 16	Self-service endpoint with email verification; returns current data for review and queues correction
Right to erasure	Art. 17	Self-service endpoint with email verification; anonymises all PII across all data stores; deactivates authentication accounts
Right to restrict processing	Art. 18	Unsubscribe endpoint; DSAR flow
Right to data portability	Art. 20	Self-service endpoint; returns all personal data in machine-readable JSON
Right to object	Art. 21	Unsubscribe endpoint
Withdraw consent	Art. 7(3)	Unsubscribe endpoint; consent withdrawal endpoint; DSAR erasure
Automated decision-making	Art. 22	Not applicable – all assessment outputs are advisory; no automated decisions with legal effect

1.5.1 Safeguards

- **Email verification:** All DSAR requests require email verification before any data is disclosed (Art. 12(6))
- **Token security:** Verification tokens expire after 24 hours and are single-use
- **Rate limiting:** Request limits per email and per IP address prevent abuse
- **Audit trail:** Every DSAR request is logged for compliance evidence (no PII in log entries)
- **Response time:** Automated processing ensures responses within minutes, well within the Art. 12(3) one-month deadline

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

1.5.2 Exceptions to Erasure (Art. 17(3))

The right to erasure does not apply to data required for compliance with a legal obligation (e.g., DSAR audit records) or for the establishment, exercise, or defence of legal claims.

1.6 Breach Notification

1.6.1 Art. 33 – Notification to Supervisory Authority

SettlDay commits to notifying the relevant supervisory authority within **72 hours** of becoming aware of a personal data breach. The notification includes the nature of the breach, categories and approximate number of data subjects and records affected, likely consequences, and measures taken or proposed.

1.6.2 Art. 34 – Notification to Data Subjects

Where a breach is likely to result in a high risk to the rights and freedoms of data subjects, affected individuals are notified directly via email with a clear, plain-language description of the breach, the personal data affected, recommended protective steps, and SettlDay's response measures.

1.6.3 Breach Register

A breach register is maintained in accordance with Art. 33(5), recording all breaches including those assessed as not requiring supervisory authority notification.

1.7 International Data Transfers

1.7.1 Current Transfer Posture

Transfer	Mechanism	Status
Infrastructure hosting (EU)	All data stored in EU; no transfer outside EU	Active
AI inference (EU)	AWS Bedrock EU regions only; data never leaves the EU	Active
Email delivery (EU)	EU-based provider; no international transfer	Active
Payment processing (US)	Stripe DPA with EU Standard Contractual Clauses	Active

All SettlDay infrastructure is located within the European Union. The only transfer outside the EU is to Stripe for payment processing, which is governed by a signed Data Processing Agreement incorporating EU Standard Contractual Clauses.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

> **Note on AI Provider:** Anthropic does not process SettlDay customer data. AI models are invoked via AWS Bedrock (AWS EMEA SARL, Luxembourg). The processor relationship is with AWS, not Anthropic. Anthropic is not a sub-processor.

1.8 Data Protection Officer Status

A formal Data Protection Officer is **not required**. SettlDay processes primarily organisational (B2B) data – professional contact details and firm-level operational metrics. The GDPR Art. 37 thresholds for mandatory DPO appointment are not met:

- SettlDay does not carry out large-scale systematic monitoring of individuals
- SettlDay does not process special category data at scale

German BDSG Section 38 is also not triggered.

1.9 Data Protection Contact

Email	privacy@settlday.com
Postal	amalics GmbH, Simrockstr. 23, 80997 Munchen, Germany

The data protection contact handles all data protection inquiries, DSAR requests, and supervisory authority correspondence.

1.10 Supervisory Authority

Lead supervisory authority: Bayerisches Landesamt fur Datenschutzaufsicht (BayLDA) – the competent data protection authority for private companies established in Bavaria, Germany.

1.11 Technical and Organisational Measures

SettlDay maintains comprehensive technical and organisational measures under Art. 32, including:

- **Encryption:** TLS in transit; AES-256 at rest on all storage
- **Authentication:** JWT-based authentication via a self-hosted identity provider
- **Authorisation:** Role-based access control with least-privilege enforcement
- **Tenant isolation:** Dual-layer isolation (database-level and application-level) prevents cross-tenant data access
- **Input validation:** Strict schema validation on all API inputs

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

- **Rate limiting:** Global and per-endpoint rate limiting with fail-closed behaviour on sensitive endpoints
- **PII detection:** Multi-layer data minimisation pipeline scrubs personal identifiers before AI processing
- **Audit trail:** Timestamps and actor identifiers on all records; immutable audit log for security and compliance events
- **Log hygiene:** Structured logging with automated PII scrubbing
- **Automated retention:** Daily enforcement of all data retention periods
- **Incident response:** Five documented incident response playbooks covering service outage, authentication attack, account compromise, data breach, and supply chain incident

---

The full internal GDPR compliance documentation, including the Art. 30 ROPA, is available under NDA on request. Contact privacy@settlday.com.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

2. Data Flow Architecture

Document ID	TC-ARCH-001
Classification	Public – Trust Center

2.1 Quick Facts

Question	Answer
Where is my data stored?	EU only
Is my data used to train AI models?	Never
Is my firm name sent to the AI?	Never
How long does the AI provider retain my data?	Zero – inference logging is disabled on AWS Bedrock
Which AI provider handles my data?	AWS Bedrock (EU regions) – not Anthropic directly
Can I delete my data?	Yes – self-service deletion, hard delete within 30 days

2.2 Data Flow Steps

2.2.1 Step 1 – Your Assessment Data

Assessment responses, firm profile data, and uploaded documents are transmitted over TLS and stored encrypted (AES-256) on EU infrastructure.

What is stored at this stage:

- Firm type, size, and jurisdictions of operation
- Assessment question responses and maturity scores
- Operational KPIs (fail rates, STP rates) if provided
- Free-text comments (if entered)
- Uploaded document content (temporary – see Step 2)

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

2.2.2 Step 2 – Data Minimisation and Pseudonymisation

Before any data is sent to an AI system, SettlDay applies the following transformations entirely on its own EU infrastructure:

Transformation	Detail
Firm name removed	Your firm's name is stripped from all data before AI processing and never transmitted to the AI provider
Documents summarised	Uploaded documents are reduced to short structured excerpts on SettlDay servers; original files are deleted after extraction
PII replaced	Names, email addresses, and other personal identifiers in free-text fields and document excerpts are replaced with anonymous placeholders
Minimum data forwarded	Only the data fields required to generate the report are included – no identifiers, no account metadata

The result is a pseudonymised, firm-name-free payload containing only what is necessary for the AI to generate a relevant report.

2.2.3 Step 3 – AI Processing

The pseudonymised payload is sent to **AWS Bedrock**, Amazon's managed AI inference service, operating exclusively in EU regions.

Property	Detail
Infrastructure owner	Amazon Web Services EMEA SARL (EU entity, Luxembourg)
Data residency	EU regions only – no data leaves the EU
Inference logging	Disabled – inputs and outputs are not logged or stored by AWS
Training use	Never – AWS Bedrock contractual terms prohibit use of customer data for model training or improvement
Anthropic's role	None – Anthropic does not receive, process, see, or store any customer data when models run on Bedrock. The processor relationship is with AWS, not Anthropic

> **Why Bedrock?** SettlDay uses AWS Bedrock specifically because it provides EU data residency, disabled inference logging, and a formal GDPR Data Processing Addendum – guarantees that are not available on the AI model provider's direct API. This is a deliberate architectural choice to meet EU data residency and zero-retention requirements.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

2.2.4 Step 4 – Your Report

The raw AI output is returned to SettlDay's EU servers. Post-processing on SettlDay infrastructure:

- Re-inserts your firm name and relevant contextual details
- Validates and sanitises the AI output
- Structures the report into sections (PDF)
- Stores the final report encrypted on SettlDay's EU infrastructure

Your report is only ever assembled in complete form on SettlDay's own servers. The AI never sees your firm name or personal details – they are added only after the AI has finished processing.

2.3 Compliance Framework

Obligation	Status	Detail
GDPR Art. 30 – ROPA	Maintained	Full records of processing activities documented
Data Processing Agreement	Available	DPA with EU Standard Contractual Clauses available for enterprise customers
DPIA	Completed	Data Protection Impact Assessment completed and signed
Self-service data deletion	Implemented	Account deletion with grace period followed by hard delete of all personal data
Data portability	Implemented	Full JSON export of all personal data available
EU AI Act – transparency	Compliant	AI-assisted report generation disclosed to users; no high-risk AI system classification
Breach notification	72-hour commitment	Supervisory authority notified within 72 hours of discovery (GDPR Art. 33)
Data subject rights	Implemented	Art. 15-22 procedures documented and self-service where possible

2.4 Data Flow Summary

Stage	What happens	Where	Data exposed to AI?
1. Collection	Assessment responses and documents submitted via TLS	SettlDay EU	No
		SettlDay EU	No

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

Stage	What happens	Where	Data exposed to AI?
2. Pre-processing	Firm name removed, PII replaced with placeholders, documents summarised		
3. AI inference	Pseudonymised payload sent to AWS Bedrock	AWS Bedrock EU	Only anonymised data – no PII, no firm name
4. Post-processing	Firm name re-inserted, report validated and rendered as PDF	SettlDay EU	No
5. Delivery	Encrypted report stored and delivered to user	SettlDay EU	No

---

2.5 EU Data Residency

All data remains within the EU at every stage of processing:

Data Category	Location	Leaves EU?
Firm name and identity	SettlDay EU servers only	No – never transmitted to any third party
User personal data (name, email, credentials)	SettlDay EU infrastructure	No
Raw assessment responses	SettlDay EU database (encrypted)	No
Uploaded documents	SettlDay EU servers (deleted after summarisation)	No
Generated reports	SettlDay EU database (encrypted)	No
Pseudonymised AI payload (no PII, no firm name)	SettlDay EU servers and AWS Bedrock EU	No – stays within EU AWS regions
Payment data	Stripe (US, EU SCCs in effect)	Card data handled by Stripe.js – never touches SettlDay servers

Anthropic has zero data access. Claude runs on AWS Bedrock managed infrastructure; the processor relationship is with AWS.

The full Sub-Processor Register is included in the Vendor Due Diligence Pack, available at the SettlDay Trust Center. For questions about data flows, contact privacy@settlday.com.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

3. Data Protection Impact Assessment – Summary

Document ID	TC-DPIA-001
Classification	Public – Trust Center

3.1 Data Controller

Entity	amalics GmbH (trading as SettlDay)
Address	Simrockstr. 23, 80997 Munchen, Germany
Registration	HRB 264611, Amtsgericht Munchen
Data protection contact	privacy@settlday.com

3.2 Processing Activities Overview

This DPIA was conducted under GDPR Art. 35 to assess the data protection risks arising from SettlDay's processing of personal data, with particular focus on the AI report generation pipeline. SettlDay is a B2B SaaS platform that helps mid-market financial firms prepare for T+1 settlement transition.

The following processing activities are covered:

Processing Activity	Description	Legal Basis
User account management	Registered user accounts for platform access	Art. 6(1)(b) – Contract
Assessment data collection	Structured questionnaire capturing firm readiness across operational categories	Art. 6(1)(b) – Contract
Document upload	Extraction of relevant operational information from uploaded documents to personalise reports	Art. 6(1)(b) – Contract
AI report generation	Personalised T+1 readiness reports generated via a large language model on AWS Bedrock EU	Art. 6(1)(b) – Contract
		Art. 6(1)(a) – Consent

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Processing Activity	Description	Legal Basis
Report request flow	Unauthenticated users complete an assessment and provide contact details to receive a report	
Waitlist registration	Pre-registration of interest for early platform access	Art. 6(1)(a) – Consent
Customer support	Handling of support inquiries via self-hosted support platform on EU infrastructure	Art. 6(1)(b) – Contract / Art. 6(1)(f) – Legitimate interest
DSAR processing	Fulfilment of data subject rights under Art. 15-22	Art. 6(1)(c) – Legal obligation

3.3 Necessity and Proportionality

3.3.1 Necessity

Each processing activity is necessary for the delivery of SettlDay's core services. Assessment data is required to generate personalised readiness reports. Contact details are required to deliver reports. The AI pipeline is necessary to produce the depth of analysis that static scoring cannot achieve.

3.3.2 Proportionality

Principle	Implementation
Data minimisation (Art. 5(1)(c))	Assessment sessions are anonymous by default; PII is only collected when the user explicitly requests a report. For AI processing: firm name is excluded, PII is detected and scrubbed, and documents are summarised before forwarding. Only the minimum data required to generate the report is sent to the AI provider.
Purpose limitation (Art. 5(1)(b))	Contact data collected for report delivery is not used for marketing unless explicit follow-up consent is given. AI processing data is used solely for report generation. The AI provider's contractual terms prohibit use of customer data for model training.
Storage limitation (Art. 5(1)(e))	Retention periods are defined per data category with automated daily enforcement. Expired PII is anonymised automatically. The AI provider retains no data – inference logging is disabled. Original uploaded documents are deleted immediately after extraction.
Accuracy (Art. 5(1)(d))	Data subjects can submit self-service rectification requests with email verification.

3.3.3 Alternatives Considered

Alternatives such as fully anonymous assessments, direct AI provider APIs (lacking EU data residency guarantees), and sending firm names to the AI were evaluated and rejected in favour of the current privacy-preserving architecture.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

3.4 Risk Assessment Summary

3.4.1 Risk Matrix

Risk	Residual Risk Level
Unauthorised access to PII	Medium (mitigated by tenant isolation, authentication, rate limiting)
Data breach via injection attack	Medium (mitigated by parameterised queries, input validation, security headers)
Cross-tenant data leakage	Medium (mitigated by dual-layer tenant isolation at database and application level)
Third-party AI processor breach	Low (inference logging disabled; no data retained; firm name and PII excluded from all AI payloads)
PII leakage in AI prompt	Low (mitigated by three independent pre-processing controls)
Excessive data retention	Very Low (automated daily retention enforcement)
Automated profiling concerns (Art. 22)	Low (assessment is advisory only; no automated decisions with legal effect)

3.4.2 Risk to Data Subjects

The personal data processed falls into two categories:

Platform data: Limited to professional contact information (name, email, company, job title) and firm-level business data. This data is not special category data (Art. 9), not financial data of individuals, and all data subjects interact in their professional capacity.

AI pipeline data: After pre-processing controls are applied, no directly identifying information is transmitted to the AI provider. Firm name is always excluded. PII is replaced with placeholders. Documents are summarised on SettlDay servers with originals deleted.

3.5 Key Mitigations

3.5.1 Technical Measures

- **Encryption:** TLS in transit; AES-256 at rest on all storage
- **Access control:** JWT-based authentication via self-hosted identity provider; role-based access control with least-privilege enforcement
- **Tenant isolation:** Dual-layer isolation at database level (row-level security) and application level prevents cross-tenant data access

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

- **PII detection pipeline:** Automated detection and replacement of personal identifiers in free-text and documents before any AI processing
- **Firm name exclusion:** Firm identity stripped from all AI payloads; re-inserted post-generation on SettlDay servers only
- **Document summarisation:** Uploaded documents reduced to structured excerpts on SettlDay EU servers before AI processing; originals deleted after extraction
- **Inference logging disabled:** The AI provider does not log or retain inputs or outputs after inference
- **Audit trail:** Timestamps and actor identifiers on all records; immutable audit log for compliance events
- **Automated retention:** Daily enforcement of all retention periods with automatic anonymisation of expired PII
- **DSAR email verification:** Cryptographically random, time-limited, single-use tokens required before any data disclosure
- **PII scrubbing in logs:** Automated redaction of personal data patterns from all structured log output

3.5.2 Organisational Measures

- Data protection contact at privacy@settlday.com
- Privacy policy published
- Data processing agreements in effect with all sub-processors
- Five documented incident response playbooks
- Breach notification procedure with 72-hour timeline (Art. 33/34)
- Annual GDPR awareness training programme

3.6 Data Protection Officer Status

A formal DPO is **not required**. SettlDay processes primarily organisational (B2B) data – professional contact details and firm-level operational metrics. The GDPR Art. 37 thresholds for mandatory DPO appointment are not met. German BDSG Section 38 is also not triggered.

Data protection contact: privacy@settlday.com

3.7 Conclusion

3.7.1 Residual Risk Assessment

After applying the technical, organisational, and contractual measures described above, the residual risk to data subjects is assessed as **LOW**.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

Justification:

- Personal data processed is limited to professional contact information and pseudonymised firm-level operational data
- No special category data is processed
- Assessment data is anonymous by default; PII only collected on explicit request
- Three independent pre-processing controls applied before any data reaches the AI provider
- AWS Bedrock EU is used specifically for EU data residency and zero-retention properties; the AI model provider never receives customer data
- Multi-layered security controls (tenant isolation, authentication, rate limiting, input validation)
- Data subject rights implemented via automated, self-service endpoints
- Incident response procedures documented with GDPR-specific breach notification timelines

3.7.2 Recommendation

This DPIA concludes that the processing may proceed **without prior consultation with the supervisory authority** (Art. 36). All pre-production requirements have been satisfied.

3.7.3 Approval

The full DPIA was reviewed and signed on 2026-03-22 by the data controller's authorised representative.

The full signed DPIA is available under NDA on request. Contact privacy@settlday.com.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

4. SOC 2 Controls Overview

Document ID	TC-SOC2-001
Classification	Public – Trust Center

4.1 Overview

amalics GmbH (trading as SettlDay) is preparing for a **SOC 2 Type II audit**. All controls described in this document are implemented and documented. The Type II observation period and formal audit engagement are planned for Q4 2026 / Q1 2027.

This document summarises SettlDay's controls across the five AICPA Trust Services Criteria for prospective clients and their compliance teams.

4.2 Trust Services Criteria Coverage

4.2.1 Security

Security controls protect information and systems against unauthorised access, unauthorised disclosure of information, and damage to systems.

- **Access controls:** Authentication via self-hosted identity provider with multi-factor authentication support; role-based access control (RBAC) with least-privilege enforcement; quarterly access reviews
- **Encryption:** TLS encryption for all data in transit; AES-256 encryption at rest on all storage layers
- **Vulnerability management:** Automated static analysis security testing (SAST), dynamic application security testing (DAST) via OWASP ZAP and Nuclei on a weekly schedule, container scanning, dependency vulnerability scanning (pip-audit for Python, npm audit for Node.js), and secret detection in CI/CD pipelines; vulnerability remediation SLAs defined by severity
- **Incident response:** Five documented incident response playbooks covering service outage, authentication attack, account compromise, data breach, and supply chain incident; severity classification with defined response times
- **Network security:** Security headers (HSTS, CSP, X-Frame-Options, Permissions-Policy); rate limiting at infrastructure and application layers; network segmentation via Kubernetes network policies

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

4.2.2 Availability

Availability controls ensure that the system is available for operation and use as committed or agreed.

- **Automated backups:** Automated daily database backups with point-in-time recovery, encrypted at rest
- **Disaster recovery:** Documented Business Continuity and Disaster Recovery (BCDR) plan with defined recovery objectives; provider-portable architecture enables infrastructure rebuild on alternative providers
- **Monitoring:** Metrics collection, log aggregation, and alerting dashboards with defined thresholds for service health, authentication failures, and error rates
- **Capacity management:** Documented capacity planning with auto-scaling and capacity alert rules

4.2.3 Processing Integrity

Processing integrity controls ensure that system processing is complete, valid, accurate, timely, and authorised.

- **Input validation:** Strict schema validation on all API inputs with type checking, field length limits, and pattern validation
- **Financial precision:** Financial calculations use exact decimal arithmetic; monetary values stored as integer units to prevent rounding errors
- **Audit trails:** Timestamps and actor identifiers recorded on all data records; immutable audit log for security and compliance events
- **Automated testing:** Comprehensive test suite with high coverage targets; CI/CD pipeline enforces all tests pass before deployment
- **Error handling:** Structured error handling with custom exception hierarchy; error monitoring and alerting

4.2.4 Confidentiality

Confidentiality controls protect information designated as confidential.

- **Tenant isolation:** Dual-layer isolation at database level (row-level security policies) and application level prevents cross-tenant data access
- **Data classification:** Four-tier classification scheme (Public, Internal, Confidential, Restricted) with defined handling requirements per level
- **Encryption at rest:** AES-256 encryption on all persistent storage layers including database, object storage, and block storage
- **Secrets management:** Application secrets encrypted at rest in version control and in the runtime environment; credential fields use secure types to prevent accidental logging or serialisation

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

4.2.5 Privacy

Privacy controls address the collection, use, retention, disclosure, and disposal of personal information.

- **GDPR compliance:** Full compliance with the General Data Protection Regulation, including records of processing activities (ROPA), Data Protection Impact Assessment (DPIA), and data processing agreements with all sub-processors
- **Data retention automation:** Automated daily enforcement of retention periods; expired personal data anonymised automatically
- **DSAR implementation:** Self-service, email-verified endpoints for data access (Art. 15), erasure (Art. 17), and portability (Art. 20) requests
- **Consent management:** Post-login consent gate with versioned consent text, explicit acknowledgement, and full audit trail
- **PII protection:** Multi-layer data minimisation pipeline scrubs personal identifiers before AI processing; structured log output automatically redacts PII patterns

---

4.3 Security Controls Summary

Control Area	Implementation
Authentication	Self-hosted identity provider with OAuth 2.0 and PKCE; JWT validation with RS256 signature verification; short-lived access tokens in HttpOnly cookies
Authorisation	Role-based access control with role hierarchy (viewer, admin, owner); authorisation enforced on all write endpoints
Encryption in transit	TLS on all external traffic; HSTS enforced; database connections encrypted with certificate verification
Encryption at rest	AES-256 on all storage layers (database, object storage, block storage); secrets encrypted via authenticated encryption
Tenant isolation	Database-level row-level security policies combined with application-level organisation filtering; every tenant-scoped query automatically filtered
Input validation	Strict schema validation with type checking, field length limits, pattern matching, and enum validation on all API inputs
Rate limiting	Infrastructure-level and per-endpoint rate limiting; fail-closed behaviour on sensitive endpoints (returns error if rate limiting infrastructure is unavailable)
Security headers	HSTS, Content-Security-Policy, X-Frame-Options (DENY), X-Content-Type-Options, Referrer-Policy, Permissions-Policy
Audit logging	Timestamps and actor identifiers on all records; immutable audit log for security and compliance events; structured security event logging
PII scrubbing	

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Control Area	Implementation
	Automated redaction of personal data patterns from all structured log output; multi-layer PII detection before AI processing
Vulnerability scanning	Automated SAST, container scanning, dependency scanning (pip-audit for Python, npm audit for Node.js), and secret detection in CI/CD; blocking on critical and high severity findings
Incident response	Five documented playbooks with severity classification, defined response SLAs, evidence preservation procedures, and GDPR-specific notification steps

---

4.4 Development Practices

- **Automated testing:** Comprehensive test suite executed on every pull request and push; high coverage targets enforced
- **Code review:** All changes require pull request review before merge; CI must pass before merge is permitted
- **CI/CD pipeline:** Automated testing, linting, formatting, security scanning (SAST, container scanning, dependency scanning via pip-audit and npm audit, secret detection) on every change
- **Pre-commit hooks:** Automated code formatting, linting, and secret detection before code is committed
- **Pre-push hooks:** Full test suite gate before code is pushed
- **Change management:** Formal change management policy with escalating approval and testing requirements based on change risk level
- **Secure coding standards:** Documented secure coding standards enforced through tooling; parameterised queries exclusively (no raw SQL); financial calculations use exact decimal arithmetic

---

For questions about SettlDay's SOC 2 readiness or to request additional control documentation, contact privacy@settlday.com.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

5. Information Security Overview

Document ID	TC-ISP-001
Classification	Public – Trust Center

5.1 Purpose

This document provides a public extract of the SettlDay Information Security Policy. The policy establishes the information security requirements for the SettlDay platform, a B2B SaaS application that helps mid-market financial firms prepare for T+1 settlement transition.

Given the sensitive nature of financial services data processed by the platform, SettlDay maintains controls to protect the confidentiality, integrity, and availability of all information assets in accordance with SOC 2 Trust Services Criteria, GDPR, and industry expectations for financial technology platforms.

5.2 Scope

The Information Security Policy applies to:

- **All personnel:** Employees, contractors, and third-party vendors with access to SettlDay systems, data, or infrastructure
- **All environments:** Production, staging, development, CI/CD pipelines, and local development environments
- **All information assets:** Source code, customer data, authentication credentials, infrastructure configurations, and operational data

5.3 Security Governance

- **Executive oversight:** The CEO approves the information security policy and allocates resources for security initiatives
- **CTO ownership:** The CTO owns and maintains the information security policy, serves as Incident Commander for security incidents, and conducts quarterly security reviews
- **Regular reviews:** Quarterly security controls effectiveness reviews; annual full policy review; semi-annual risk assessment updates
- **Policy review cycle:** All governance documents are reviewed annually with version control and approval tracking

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

5.4 Asset Management and Data Classification

SettlDay classifies information assets into four levels with defined handling requirements:

Level	Definition	Handling Requirements
Restricted	Data whose unauthorised disclosure would cause severe harm; regulatory notification required on breach	Encrypted at rest and in transit; access limited to minimum necessary personnel; logged access
Confidential	Internal data whose disclosure would cause moderate harm	Encrypted in transit; access controlled by role; no sharing outside organisation without NDA
Internal	Data intended for internal use only	Access limited to employees and authorised contractors
Public	Data intended for public consumption	No restrictions on distribution

All customer assessment data, user personal data, and authentication credentials are classified as **Restricted**.

5.5 Access Management

5.5.1 Authentication

- Self-hosted identity provider with OAuth 2.0 and PKCE (RFC 7636)
- JWT access tokens validated via JWKS with RS256 signature verification
- Short-lived access tokens in HttpOnly cookies with SameSite attributes
- Multi-factor authentication support
- Rate limiting on authentication endpoints

5.5.2 Authorisation

- Role-based access control (RBAC) with role hierarchy (viewer, admin, owner)
- Authorisation enforced on all write endpoints with detailed logging of authorisation failures
- Least-privilege principle: users receive the minimum access necessary for their role

5.5.3 Multi-Tenant Isolation

- Database-level row-level security policies automatically filter every tenant-scoped query
- Application-level organisation filtering as defence-in-depth
- No single user can access data belonging to another organisation

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

5.5.4 Access Reviews

- Quarterly access reviews covering all systems and infrastructure
- Documented access review procedures with offboarding checklists
- Separation of duties enforced through CI/CD pipeline controls

---

5.6 Network Security

5.6.1 Encryption in Transit

- TLS encryption on all external traffic with automatic certificate management
- HSTS (HTTP Strict Transport Security) enforced with preload
- Database connections encrypted with certificate verification
- Email delivery via STARTTLS

5.6.2 Security Headers

All API responses include comprehensive security headers:

- **Strict-Transport-Security** – enforces HTTPS connections
- **Content-Security-Policy** – prevents cross-site scripting and injection attacks
- **X-Frame-Options** – prevents clickjacking (set to DENY)
- **X-Content-Type-Options** – prevents MIME-type sniffing
- **Referrer-Policy** – controls referrer information leakage
- **Permissions-Policy** – restricts browser feature access (camera, microphone, geolocation disabled)

5.6.3 Web Application Firewall

- Rate limiting at infrastructure and application layers
- Request body size limits enforced
- Server version information suppressed

5.7 Data Protection

5.7.1 Encryption at Rest

AES-256 encryption at rest on all persistent storage layers including database, object storage, and block storage volumes. Application secrets are encrypted via authenticated encryption schemes.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

5.7.2 PII Detection Before AI Processing

A multi-layer data minimisation pipeline processes all data before it reaches any AI system:

- **Layer 1:** Automated detection and replacement of personal identifiers in free-text and documents
- **Layer 2:** Firm name stripped from all AI payloads; re-inserted post-generation on SettlDay servers only
- **Layer 3:** Uploaded documents summarised on SettlDay EU servers; originals deleted after extraction

5.7.3 Structured Log Scrubbing

All structured log output is automatically scanned for personal data patterns, which are redacted before logs are written. This prevents accidental PII exposure in monitoring and log aggregation systems.

5.7.4 Automated Retention Enforcement

Data retention periods are enforced by a daily automated process that anonymises or purges personal data that has exceeded its defined retention period.

5.8 Incident Response

SettlDay maintains five documented incident response playbooks:

Playbook	Scope
Service Outage	Platform availability incidents and recovery procedures
Authentication Attack	Detection, containment, and forensics for brute force and credential stuffing
Account Compromise	Isolation, credential rotation, and impact assessment for compromised accounts
Data Breach	Personal data breach response including GDPR Art. 33/34 notification procedures
Supply Chain Incident	Third-party compromise assessment, containment, and vendor notification

5.8.1 Response SLAs

Severity	Response Time	Communication Cadence
Critical	15 minutes	Every 30 minutes

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Severity	Response Time	Communication Cadence
High	1 hour	Every 2 hours
Medium	4 hours	Daily
Low	24 hours	Weekly

5.8.2 Evidence Preservation

Incident response procedures include evidence preservation steps, structured incident timelines, root cause analysis, and post-incident reviews conducted within 5 business days of significant incidents.

5.9 Business Continuity

- **Automated backups:** Automated daily database backups with point-in-time recovery, encrypted at rest
- **Disaster recovery:** Documented BCDR plan designed for rapid recovery; provider-portable architecture enables infrastructure rebuild on alternative cloud providers
- **Source code redundancy:** Full version history maintained on hosted repository with geographic redundancy
- **Container images:** Versioned, immutable container images stored in a private registry

---

5.10 Vendor Management

- **Third-party risk assessment:** Formal vendor risk assessment framework with vendor classification, assessment criteria, and monitoring requirements
- **Sub-processor monitoring:** All sub-processors have data processing agreements in effect; annual vendor risk reviews
- **Sub-processor change notification:** 30 calendar days' prior written notice before engaging any new sub-processor; client right of objection within 15 days

---

5.11 Compliance

Framework	Applicability
GDPR	Full compliance – DPIA completed, ROPA maintained, DSAR endpoints implemented, automated retention enforcement
EU AI Act	Limited risk classification – transparency obligations met, AI-generated content disclosed to users

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Framework	Applicability
DORA	SettlDay is an ICT third-party service provider under Art. 3(21); contractual provisions addressing Art. 28-30 requirements in preparation
SOC 2 Type II	Audit in preparation – controls implemented and documented across all five Trust Services Criteria

5.12 Vulnerability Management

- **Automated SAST:** Static analysis security testing on every code change, covering established security vulnerability patterns
- **Container scanning:** Container images scanned for vulnerabilities before deployment; critical and high findings block deployment
- **Dependency scanning:** All dependencies scanned for known CVEs on every change using pip-audit (Python) and npm audit (Node.js)
- **Secret detection:** Automated scanning for leaked credentials in code changes and pre-commit hooks
- **Automated DAST:** Dynamic Application Security Testing using OWASP ZAP (full scan) and Nuclei on a weekly schedule; findings reviewed and triaged against vulnerability remediation SLAs

5.12.1 Vulnerability Remediation SLAs

Severity	Remediation Deadline
Critical (CVSS 9.0-10.0)	24 hours
High (CVSS 7.0-8.9)	72 hours
Medium (CVSS 4.0-6.9)	30 days
Low (CVSS 0.1-3.9)	Next release cycle

The full Information Security Policy is available under NDA on request. Contact privacy@settlday.com.

© 2026 SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

6. Sub-Processor Register

Document ID	SUB-PROC-001
Classification	Public — Trust Center

6.1 Controller

amalics GmbH Simrockstr. 23, 80997 München, Germany Registered at Amtsgericht München, HRB 264611

SettlDay is a joint initiative by **Kommalpha AG** (Am Ortfelde 38 C, 30916 Isernhagen, HRB 204586) and **amalics GmbH**.

6.2 Sub-Processors Engaged in the Provision of SettlDay

Sub-Processor	Purpose	Data Processed	Processing Location	DPA Status
DigitalOcean, LLC	Cloud infrastructure (compute, managed database)	All platform data (encrypted at rest, AES-256)	Frankfurt, EU	In effect via DigitalOcean Data Processing Agreement
Amazon Web Services EMEA SARL	AI inference via AWS Bedrock	Pseudonymised assessment data only — no PII and no firm names are transmitted	Frankfurt, EU (eu-central-1)	In effect via AWS GDPR Data Processing Addendum including EU Standard Contractual Clauses
IONOS SE	Transactional email delivery	Email addresses (in transit only)	Germany	In effect via IONOS Data Processing Agreement
Stripe, Inc.	Payment processing	Payment card data (never touches SettlDay servers — handled entirely by Stripe.js on the client side)	United States (EU Standard Contractual Clauses in effect)	Stripe Data Processing Agreement signed

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

Sub-Processor	Purpose	Data Processed	Processing Location	DPA Status
FusionAuth, Inc.	User authentication software	N/A — self-hosted on SettlDay's own EU infrastructure; no data leaves SettlDay systems	Frankfurt, EU	N/A — no Data Processing Agreement required (self-hosted software, FusionAuth does not process data)

6.3 Note on AI Provider

Anthropic, PBC is **not** a sub-processor. SettlDay accesses Anthropic's Claude language model exclusively through AWS Bedrock, a managed inference service operated by Amazon Web Services within the EU. Anthropic does not receive, store, or process any SettlDay data. The AWS Bedrock relationship is covered by the AWS Data Processing Addendum listed above.

6.4 Sub-Processor Change Notification

amalics GmbH commits to providing **30 calendar days' prior written notice** before engaging any new sub-processor or materially changing the scope of processing by an existing sub-processor.

Clients have the **right to object within 15 calendar days** of receiving such notification. If a client raises a justified objection, amalics GmbH will work with the client to find a mutually acceptable solution. If no resolution can be reached, the client may terminate the affected services.

6.5 Contact

For sub-processor change notifications, questions, or to register for update alerts:

privacy@settlday.com

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

7. Vendor Security Questionnaire — SettlDay

Document ID	VSQ-001
Classification	Public — Trust Center

This pre-filled questionnaire provides answers to common vendor due diligence questions from regulated financial institutions. For questions not covered here, please contact **privacy@settlday.com**.

7.1 Company Information

1.1 What is the legal name and registration of the service provider? amalics GmbH, registered at Amtsgericht München, HRB 264611. SettlDay is a joint initiative by amalics GmbH and Kommalpha AG (Amtsgericht Hannover, HRB 204586).

1.2 What is the registered address? amalics GmbH, Simrockstr. 23, 80997 München, Germany.

1.3 What is the address of the content partner? Kommalpha AG, Am Ortfelde 38 C, 30916 Isernhagen, Germany.

1.4 In which jurisdiction is the company incorporated? Germany (Federal Republic of Germany).

1.5 Who is the data protection contact? privacy@settlday.com

1.6 What is the nature of the service provided? SettlDay is an advisory assessment platform for T+1 settlement readiness. It provides advisory reports, regulatory research, and readiness dashboards for mid-market financial firms preparing for T+1 settlement transition. All outputs are advisory and require human review.

1.7 How long has the company been operating? amalics GmbH has been operating since its registration. SettlDay is actively developed and in service.

1.8 Does the company carry professional indemnity or cyber liability insurance? Yes. Details available on request.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

7.2 Data Protection & Privacy

2.1 Is the service GDPR-compliant? Yes. SettlDay is designed and operated in full compliance with the General Data Protection Regulation (EU) 2016/679.

2.2 Has a Data Protection Officer (DPO) been designated? A DPO designation is not required under Art. 37 GDPR for amalics GmbH based on the nature and scale of processing activities. The data protection contact is privacy@settlday.com.

2.3 What is the legal basis for processing personal data? The primary legal bases are: (a) performance of a contract (Art. 6(1)(b) GDPR) for service delivery; (b) legitimate interests (Art. 6(1)(f) GDPR) for security and fraud prevention; and (c) consent (Art. 6(1)(a) GDPR) where applicable (e.g., optional analytics).

2.4 What categories of personal data are processed? User account data (name, email address, organisation affiliation), authentication data, assessment responses entered by users, and usage metadata. Payment card data is handled entirely by Stripe and never touches SettlDay servers.

2.5 Has a Data Protection Impact Assessment (DPIA) been conducted? Yes. A DPIA has been conducted covering the use of AI-assisted processing. The assessment concluded that residual risks are mitigated to an acceptable level through the implemented technical and organisational measures, particularly the multi-layer data minimisation pipeline applied before AI processing.

2.6 Is personal data transferred outside the EU/EEA? No personal data is transferred outside the EU/EEA for processing. All infrastructure, databases, and AI inference run in EU data centres (Frankfurt, Germany). The sole exception is Stripe (payment processing), which operates under EU Standard Contractual Clauses, and payment card data is handled entirely on Stripe's infrastructure via client-side integration.

2.7 What is the data retention policy? Data is retained for the duration of the contractual relationship. Upon termination, client data is deleted within 30 days unless a longer retention period is required by applicable law. Clients may request data export or deletion at any time.

2.8 How are Data Subject Access Requests (DSARs) handled? DSARs are handled by the data protection contact (privacy@settlday.com). Requests are acknowledged within 72 hours and fulfilled within the statutory 30-day period. The platform supports data export functionality for efficient DSAR fulfilment.

2.9 What is the data breach notification procedure? Data breaches are assessed immediately upon detection. The supervisory authority is notified within 72 hours where required under Art. 33 GDPR. Affected data subjects and clients are notified without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

2.10 Is a Data Processing Agreement (DPA) available? Yes. A DPA conforming to Art. 28 GDPR is available and provided as part of the contractual framework. It includes the Technical and Organisational Measures (TOM-001) as an annex.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

2.11 Are data processing records maintained under Art. 30 GDPR? Yes. Records of processing activities are maintained and available for inspection by supervisory authorities.

2.12 How is user consent managed? A consent management mechanism is implemented within the platform. Users are presented with clear consent requests at the point of data collection. Consent can be withdrawn at any time.

7.3 Information Security

3.1 Does the organisation maintain a formal information security policy? Yes. An information security policy is maintained, reviewed regularly, and covers access control, incident response, data handling, and acceptable use.

3.2 What encryption is used for data in transit? TLS 1.2 or higher on all connections. Unencrypted connections are rejected.

3.3 What encryption is used for data at rest? AES-256 encryption for all stored data, including database storage and backups.

3.4 How is access to the platform controlled? Authentication is managed via a self-hosted identity provider. JWT-based session management with secure cookie handling. Multi-factor authentication is available.

3.5 How is tenant data isolated? PostgreSQL Row-Level Security (RLS) enforces tenant isolation at the database level. Every database query is scoped to the authenticated tenant, preventing cross-tenant data access regardless of application-layer logic.

3.6 What role-based access controls are in place? A hierarchical RBAC model with viewer, admin, and owner roles. Permissions are enforced at both the API and database levels. The principle of least privilege is applied throughout.

3.7 How is vulnerability management handled? Automated dependency vulnerability scanning using pip-audit (Python) and npm audit (Node.js) runs in the CI/CD pipeline. Security patches are applied promptly. The application dependencies are regularly updated and audited.

3.8 Has a penetration test been conducted? Yes. Automated Dynamic Application Security Testing (DAST) is performed on a weekly schedule using OWASP ZAP (full scan) and Nuclei vulnerability scanner. Reports are retained for 30 days. Results are available on request under NDA.

3.9 Is there a security monitoring capability? Yes. Infrastructure and application monitoring with real-time alerting on anomalies, errors, and security-relevant events.

3.10 Is there a documented incident response plan? Yes. Documented incident response playbooks define roles, escalation procedures, communication protocols, and post-incident review processes.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

3.11 How are secrets and credentials managed? Secrets are stored in environment-level secure secret management. No credentials are stored in source code. Secret scanning is part of the CI/CD pipeline.

3.12 What secure development practices are followed? Secure development lifecycle practices include code review, automated static analysis, dependency auditing (pip-audit for Python, npm audit for Node.js), and security-focused testing. All code changes undergo peer review before deployment.

3.13 How are logs managed? Structured application logging with automatic PII redaction. Logs are retained according to the data retention policy. Audit logs provide a tamper-resistant record of significant operations.

3.14 Is there a security awareness programme for staff? Yes. Team members receive security awareness guidance covering phishing, secure coding practices, and data handling procedures.

3.15 How is endpoint security managed for development devices? Development devices use full-disk encryption, screen lock policies, and current operating system versions. Administrative access to production systems requires multi-factor authentication.

7.4 AI & Automated Processing

4.1 Does the service use artificial intelligence or machine learning? Yes. SettlDay uses a large language model (LLM) for advisory report generation, regulatory research, and assessment analysis.

4.2 Which AI provider is used? AI inference is provided through a managed cloud service operating exclusively in the EU (Frankfurt, Germany). The AI provider does not retain any SettlDay data.

4.3 What data is sent to the AI provider? Only pseudonymised assessment data. A multi-layer data minimisation pipeline is applied before any data reaches the AI provider:

- Named entity recognition detects and replaces personal data with neutral placeholders.
- Organisation/firm names are systematically removed.
- Uploaded documents are summarised on SettlDay's own servers before any content is forwarded.

No PII and no firm names are transmitted to the AI provider.

4.4 Is client data used to train AI models? No. Client data is never used for model training, fine-tuning, or improvement by any party. Inference logging is disabled at the AI provider level to prevent any data retention.

4.5 Does the AI make automated decisions with legal effect? No. All AI outputs are advisory only. No automated decisions with legal or similarly significant effect are made. All AI-generated content is clearly labelled and intended for human review.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

4.6 How is the service classified under the EU AI Act? SettlDay is classified as a limited-risk AI system. It is not used in any of the high-risk categories defined in Annex III of the EU AI Act. Transparency obligations (Art. 52) are met by clearly labelling AI-generated content.

4.7 What transparency measures are in place regarding AI use? Users are informed that the platform uses AI for analysis and report generation. AI-generated content is clearly distinguished from human-authored content. The data minimisation measures applied before AI processing are documented in the Technical and Organisational Measures (TOM-001).

4.8 Can clients opt out of AI processing? The advisory reports are a core function of the service. However, clients control what data they enter into the platform, and the data minimisation pipeline ensures that only pseudonymised, summarised data reaches the AI provider.

4.9 How is AI output quality assured? AI outputs are generated based on structured inputs and validated against domain-specific criteria. Reports are designed for human review, and users are advised to apply professional judgement to all AI-assisted analysis.

7.5 Infrastructure & Operations

5.1 Where is the service hosted? All infrastructure is hosted in EU data centres located in Frankfurt, Germany.

5.2 Who is the primary infrastructure provider? A professional cloud infrastructure provider with ISO 27001 and SOC 2 certified data centres in the EU. See the Sub-Processor Register in the Vendor Due Diligence Pack at the SettlDay Trust Center.

5.3 Is the database managed or self-administered? The PostgreSQL database is a managed service provided by the infrastructure provider, including automated patching, encryption at rest, and automated backups.

5.4 How are database backups handled? Automated backups with point-in-time recovery are maintained by the managed database provider. Backups are encrypted and stored in the same EU region.

5.5 What are the availability targets? The service is designed for high availability with automated health monitoring, container orchestration with self-healing capabilities, and managed database failover. Specific SLA terms are defined in the service agreement.

5.6 How is change management handled? All changes follow a defined process: code review, automated testing, staging environment validation, and controlled production deployment. Rollback procedures are documented and tested.

5.7 What CI/CD security controls are in place? The CI/CD pipeline includes automated SAST, secret scanning, container scanning, and dependency auditing (pip-audit for Python, npm audit for Node.js). All security checks must pass before deployment is permitted.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

5.8 How are production deployments managed? Deployments are automated through a CI/CD pipeline with staging validation preceding production releases. Zero-downtime deployment strategies are employed.

5.9 Is there a separate staging environment? Yes. A dedicated staging environment is maintained that mirrors the production architecture. No production data is used in staging.

5.10 How is infrastructure access managed? Infrastructure access requires multi-factor authentication and is restricted to authorised personnel. Access is logged and reviewed regularly.

5.11 Are containers used? If so, how are they secured? Yes. Container images are built from minimal base images, scanned for vulnerabilities in the CI/CD pipeline, and run with restricted privileges. Images are rebuilt regularly to incorporate security patches.

7.6 Third-Party Risk

6.1 Is a sub-processor list available? Yes. The Sub-Processor Register is included in the Vendor Due Diligence Pack at the SettlDay Trust Center and provided as an annex to the Data Processing Agreement.

6.2 How are clients notified of sub-processor changes? amalics GmbH provides 30 calendar days' prior written notice before engaging new sub-processors or materially changing the scope of existing sub-processor processing.

6.3 Can clients object to new sub-processors? Yes. Clients have a right of objection within 15 calendar days of receiving notification. If no resolution can be reached, the client may terminate the affected services.

6.4 Do clients have audit rights? Yes. Contractual audit rights are available. amalics GmbH supports audit pooling arrangements to reduce the burden on both parties and will facilitate reasonable on-site or remote audits with appropriate notice.

6.5 Is there visibility into the sub-outsourcing chain? Yes. The Sub-Processor Register identifies all sub-processors and their purposes. Material changes in the sub-outsourcing chain are communicated through the sub-processor notification process.

6.6 How are sub-processors assessed? Sub-processors are assessed for their data protection capabilities, security certifications, contractual commitments, and compliance posture before engagement. Data Processing Agreements are established with all sub-processors that handle personal data.

7.7 Regulatory Compliance

7.1 How is SettlDay classified under MaRisk AT 9? For most regulated institutions, SettlDay qualifies as "sonstiger Fremdbezug" (third-party procurement) rather than outsourcing. Even under a

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

conservative classification, it would be non-material outsourcing (nicht wesentliche Auslagerung) as SettlDay does not perform any regulated activity. No BaFin notification is required. A detailed MaRisk AT 9 Executive Summary (MARISK-ES-001) and full classification analysis (MARISK-001) are available.

7.2 What is the DORA readiness status? SettlDay is preparing for compliance with DORA (Digital Operational Resilience Act) Chapter V requirements applicable to ICT third-party service providers. A DORA assessment document (DORA-001) is available on request.

7.3 Are BaFin audit rights supported? Yes. amalics GmbH will cooperate with BaFin and other competent supervisory authorities exercising their audit and access rights in relation to outsourced or procured services.

7.4 What is the SOC 2 certification status? SOC 2 Type II audit is in preparation. Security controls have been implemented and documented. The audit timeline will be communicated to clients.

7.5 Is ISO 27001 certification held? ISO 27001 certification is not currently held by amalics GmbH. The infrastructure providers hold ISO 27001 certifications for their data centre operations.

7.6 Is there an exit strategy? Yes. Clients can export all their data in standard formats at any time during the contractual relationship. Upon termination, a transition period is provided for orderly data migration, after which all client data is deleted.

7.7 How is regulatory change monitored? amalics GmbH monitors regulatory developments relevant to data protection, AI regulation, and financial services outsourcing requirements, and adapts its compliance posture accordingly.

7.8 Contractual

8.1 Is a Data Processing Agreement (DPA) available? Yes. A DPA conforming to Art. 28 GDPR is available. It includes the Technical and Organisational Measures (TOM-001) and the Sub-Processor Register (SUB-PROC-001) as annexes.

8.2 What is the standard service agreement structure? The contractual framework consists of: (a) Service Agreement / Terms of Service; (b) Data Processing Agreement with TOMs; (c) Sub-Processor Register; and (d) applicable regulatory addenda.

8.3 Is a DORA/MaRisk contractual addendum available? A DORA-compliant contractual addendum is in preparation and will address the requirements of DORA Chapter V, including information provisions, audit rights, and exit planning. Available on request once finalised.

8.4 Is audit pooling supported? Yes. amalics GmbH supports audit pooling arrangements, whereby multiple clients may participate in joint audits or rely on standardised audit reports, reducing costs and administrative burden for all parties.

8.5 What is the contract termination notice period? Termination notice periods are defined in the service agreement. Standard terms provide for reasonable notice periods with a data transition period following termination.

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

8.6 Is data portability guaranteed? Yes. Clients can export their data in standard, machine-readable formats at any time. Data portability rights under Art. 20 GDPR are fully supported.

8.7 What governing law applies? German law. Place of jurisdiction is München, Germany.

8.8 Are service level agreements (SLAs) available? SLA terms are defined in the service agreement and cover availability, support response times, and incident communication commitments. Details are available upon request.

7.9 Contact

For additional questions, to request detailed documents referenced in this questionnaire, or to initiate the vendor onboarding process:

privacy@settlday.com

amalics GmbH Simrockstr. 23, 80997 München, Germany HRB 264611, Amtsgericht München

© 2026 SettlDay — A joint initiative by Kommalpha AG and amalics GmbH