SettlDay

SETTLEMENT READINESS PLATFORM

GET IT DONE

MaRisk AT 9 / DORA Pack

Version dc151e3
Generated 2026-04-14

SettlDay – A joint initiative by Kommalpha AG and amalics GmbH

settlday.com

Contents

1. MaRisk AT 9 — Executive Summary for SettlDay

Document ID	MARISK-ES-001
Classification	Public — Trust Center

1.1 Purpose

This document provides a concise classification assessment of SettlDay under MaRisk AT 9 (Outsourcing) for compliance officers at regulated financial institutions. A detailed classification analysis is available on request (reference: MARISK-001).

1.2 What SettlDay Is

SettlDay is an **advisory assessment platform** for T+1 settlement readiness. It provides:

- Advisory assessment reports based on structured questionnaires
- Regulatory research and readiness dashboards
- AI-assisted analysis with human-reviewed outputs

SettlDay is a joint initiative by **Kommalpha AG** (Am Ortfelde 38 C, 30916 Isernhagen, HRB 204586) and **amalics GmbH** (Simrockstr. 23, 80997 München, HRB 264611).

1.3 What SettlDay Does NOT Do

SettlDay does **not**:

- Execute trades or settle transactions
- Provide custody or safekeeping of assets
- File regulatory reports on behalf of institutions
- Make autonomous decisions with legal or financial effect
- Process or route payments on behalf of clients
- Access client core banking or trading systems

All outputs are advisory in nature and require human review before any action is taken.

1.4 Classification Under MaRisk AT 9

1.4.1 Classification Steps

Step	Question	If No	If Yes
1	Does SettlDay perform a regulated banking or financial activity on behalf of the institution?	**Sonstiger Fremdbezug** (third-party procurement). No MaRisk AT 9 outsourcing requirements apply.	Proceed to Step 2.
2	Does the outsourced activity qualify as material (wesentlich) to the institution's operations?	**Non-material outsourcing** (nicht wesentliche Auslagerung). Standard contractual provisions sufficient. No BaFin notification required.	**Material outsourcing** (wesentliche Auslagerung). Full MaRisk AT 9 requirements apply. BaFin notification required. Unlikely for SettlDay.

1.4.2 Materiality Factors (if classified as outsourcing)

Factor (AT 9.2)	Assessment	Impact
Criticality to business operations	T+1 readiness assessment is preparatory, not operational	Low
Impact of disruption on regulatory obligations	Institution can continue all regulated activities without SettlDay	Low
Impact on risk profile	Professional contact data and firm-level metrics only — no transaction or client asset data	Low
Substitutability	Assessment can be performed internally or by alternative providers; JSON export available	High
Impact on internal control system	Advisory input to institution's own controls, not a control mechanism	Low

1.4.3 Recommended Classification

For most institutions, SettlDay will qualify as **sonstiger Fremdbezug** (third-party procurement of an ancillary, non-regulated service). This is analogous to procuring a research tool, market data terminal, or consulting report.

Even if an institution's internal policies classify SettlDay as outsourcing, it would be **non-material outsourcing** (nicht wesentliche Auslagerung) because:

- It does not perform any activity requiring a BaFin licence.
- It is not critical to the institution's ability to deliver regulated services.
- Failure or unavailability of SettlDay would not impair the institution's regulatory obligations.
- No BaFin notification is required for non-material outsourcing.

1.5 Key Risk Mitigations

Concern	SettlDay's Position
Data residency	All data stored and processed in the EU (Frankfurt, Germany)
Tenant isolation	Database-level row isolation per organisation
Encryption	AES-256 at rest, TLS 1.2+ in transit
AI data handling	Multi-layer PII removal before AI processing; no data retained by AI provider
Audit rights	Contractual audit rights available; audit pooling supported
Exit strategy	Full data export in standard formats at any time
Sub-processor transparency	Published sub-processor register with change notification

---

1.6 Related Documents

Reference	Document
MARISK-001	Full MaRisk AT 9 Classification Analysis (available on request)
DORA-001	DORA Chapter V Assessment (available on request)
TOM-001	Technical and Organisational Measures
SUB-PROC-001	Sub-Processor Register

1.7 Contact

For the full classification document, DORA assessment, or to discuss your institution's specific classification approach:

privacy@settlday.com

amalics GmbH Simrockstr. 23, 80997 München, Germany

2. DORA and MaRisk Overview

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

2.1 Purpose

This document summarises SettlDay's posture under the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554) and MaRisk AT 9 (BaFin Circular 10/2021 (BA)) for prospective clients that are EU-regulated financial entities. It is intended for use by compliance officers, outsourcing managers, and ICT risk management teams evaluating SettlDay as an ICT third-party service provider.

Service provider: amalics GmbH (trading as SettlDay) Simrockstr. 23, 80997 Munchen, Germany HRB 264611, Amtsgericht Munchen

2.2 SettlDay's Role Under DORA

2.2.1 Classification

Under DORA Art. 3(21), an **ICT third-party service provider** means an undertaking providing ICT services. SettlDay provides a cloud-based platform for settlement readiness assessment, AI-generated compliance reports, and regulatory research – all delivered as digital services over ICT infrastructure. SettlDay therefore falls within this definition when serving financial entity clients.

2.2.2 Critical ICT Provider Designation

SettlDay is **unlikely to be designated as a critical ICT third-party service provider** under DORA Art. 31, given:

- SettlDay does not provide core trading, clearing, settlement, or custody infrastructure
- The platform provides advisory assessment and reporting – not real-time operational services
- No systemic dependency exists across multiple financial entities

However, individual financial entity clients may classify SettlDay's services as supporting important or critical functions under their own ICT risk management framework (Art. 28(1)(a)), which triggers enhanced contractual and monitoring requirements.

2.3 DORA Contractual Provisions

SettlDay's contractual framework addresses the mandatory requirements of DORA Art. 28(3) and Art. 30:

Contractual Area	Coverage
Service description and SLAs	Defined service scope with formal service level targets
Data processing locations	All data stored and processed in the EU; specific locations documented
Data security provisions	Comprehensive technical and organisational measures covering availability, authenticity, integrity, and confidentiality
Incident notification	ICT incident notification with defined timeframes, in addition to GDPR breach notification
Business continuity and DR	Documented BCDR plan designed for rapid recovery; provider-portable architecture
Audit rights	Annual on-site audit right; competent authority access; audit pooling supported (see Section 8)
Exit strategy	Full data export, deletion within 30 days, transition assistance, no vendor lock-in (see Section 9)
Sub-outsourcing transparency	Full sub-processor register published; 30 days' prior notice before sub-processor changes; client right of objection
Competent authority cooperation	Confirmation of cooperation with ESAs and national competent authorities

2.3.1 Contractual Addendum

A combined **DORA/MaRisk contractual addendum** is in preparation (planned Q2 2026), consolidating all DORA Art. 30 mandatory provisions and MaRisk AT 9 outsourcing-specific clauses into a single supplementary agreement for regulated clients.

2.4 MaRisk AT 9 – Outsourcing Classification

2.4.1 Classification Guidance

Under MaRisk AT 9, the threshold question is whether SettlDay's service constitutes **outsourcing (Auslagerung)** or **third-party procurement (sonstiger Fremdbezug)**. The classification depends on how the institution uses SettlDay:

Usage Pattern	Likely Classification
SettlDay used as one input among several in the institution's own T+1 readiness programme	**Sonstiger Fremdbezug** (third-party procurement)
SettlDay reports supplement the institution's own compliance team analysis	**Sonstiger Fremdbezug** or non-material outsourcing
SettlDay relied upon as the primary assessment vehicle with limited internal analysis	**Non-material outsourcing (Auslagerung)**

For the majority of institutions, SettlDay is best classified as **sonstiger Fremdbezug** – the purchase of an advisory software tool that informs the institution's own decision-making.

2.4.2 Materiality Assessment

If classified as outsourcing, a materiality assessment under AT 9.2 is required. SettlDay's characteristics support a finding of **non-material outsourcing**:

Materiality Factor	Assessment
Criticality to business operations	Low – T+1 readiness assessment is a preparatory/advisory activity, not a core operational function
Impact of disruption on regulatory obligations	Low – if SettlDay is unavailable, the institution can continue all regulated activities; assessment can be performed manually or deferred
Impact on the institution's risk profile	Low – SettlDay processes professional contact data and firm-level operational metrics; no transaction data, client assets, or market-sensitive information
Substitutability	High – assessment activities can be performed internally; alternative advisory providers exist; no lock-in to SettlDay data formats
Impact on internal control system	Low – SettlDay outputs are advisory inputs, not a control mechanism

---

2.5 BaFin Cloud Guidance

SettlDay's posture addresses the key requirements of BaFin's "Orientierungshilfe zu Auslagerungen an Cloud-Anbieter":

BaFin Requirement	SettlDay Posture
Clear service description including cloud deployment model	SaaS platform on private cloud infrastructure; service scope documented in contractual materials

BaFin Requirement	SettlDay Posture
Data location transparency	All data in EU; AI inference in EU; locations documented in data processing agreement
Right of the institution and BaFin to audit	Covered in data processing agreement, including explicit BaFin access rights
Audit pooling	Supported – multiple institutions may conduct joint audits
Adequate exit provisions	Data export, deletion, and transition assistance documented
Encryption and key management	AES-256 at rest; TLS in transit; secrets managed via authenticated encryption

---

2.6 Sub-Outsourcing Chain

SettlDay provides full transparency into its sub-processor chain. The complete Sub-Processor Register is included in this pack and in the Vendor Due Diligence Pack at the SettlDay Trust Center. Current sub-processors:

Sub-Processor	Purpose	Location
DigitalOcean, LLC	Cloud infrastructure (compute, managed database)	Frankfurt, EU
AWS EMEA SARL	AI inference (Bedrock)	Frankfurt, EU
IONOS SE	Transactional email delivery	Germany
Stripe, Inc.	Payment processing	US (EU SCCs in effect)

SettlDay commits to: - **30 calendar days' prior written notice** before engaging new sub-processors - **Client right of objection** within 15 calendar days of notification - **Full liability** for sub-processor compliance

The full Sub-Processor Register with DPA status is included later in this pack.

2.7 Incident Response

SettlDay maintains five documented incident response playbooks with defined severity classification and response times:

Severity	Response Time
Critical	15 minutes

Severity	Response Time
High	1 hour
Medium	4 hours
Low	24 hours

Procedures include evidence preservation, structured incident timelines, root cause analysis, and post-incident reviews. GDPR Art. 33/34 breach notification procedures are integrated into the data breach playbook. DORA-specific ICT incident notification for financial entity clients is being formalised.

2.8 Audit Rights

Audit rights documented in the data processing agreement include:

- **Annual on-site audit right** with 30 days' written notice
- **BaFin and competent authority access** to SettlDay's premises, systems, and documentation
- **Audit pooling** with other institutions to reduce burden on both parties
- **SOC 2 Type II reports** provided as evidence of compliance, with residual on-site audit right preserved

---

2.9 Exit Strategy

Exit Component	Provision
Data export	Full JSON export of all institution data via self-service or on request
Data deletion	All data deleted within 30 days of request
Transition period	Contractually defined transition assistance period
No vendor lock-in	Standard data formats; no proprietary dependencies; provider-portable architecture
Deletion confirmation	Written deletion confirmation provided on request

---

2.10 Information for Client Registers

Financial entity clients maintaining an ICT third-party register under DORA Art. 28(3) can use the following:

Item	Detail
Legal entity	amalics GmbH, trading as SettlDay
Registered office	Simrockstr. 23, 80997 Munchen, Germany
Registration	HRB 264611, Amtsgericht Munchen
Jurisdiction	German law (Munich courts)
Data processing locations	EU only
Security certifications	SOC 2 Type II audit in preparation
Data protection contact	privacy@settlday.com

2.11 Regulatory References

Regulation / Guidance	Relevant Provisions
DORA (Regulation (EU) 2022/2554)	Art. 3(21) (ICT provider definition), Art. 28-30 (ICT third-party risk and contractual requirements), Art. 31 (critical provider designation)
MaRisk (BaFin Circular 10/2021 (BA))	AT 9 (Outsourcing), BT 3.4 (Outsourcing register)
BaFin Orientierungshilfe Cloud-Auslagerungen (Nov 2018)	Cloud-specific outsourcing requirements
EBA Guidelines on Outsourcing (EBA/GL/2019/02)	EU-wide outsourcing framework
KWG Section 25b	Legal basis for outsourcing requirements
KAGB Section 36	Outsourcing requirements for KVGs

2.12 Contact

For regulatory inquiries, DORA/MaRisk classification questions, or to request the full DORA implications assessment or MaRisk AT 9 classification guidance document:

privacy@settlday.com

A detailed DORA implications assessment and MaRisk AT 9 classification guidance document are available under NDA on request.

3. Sub-Processor Register

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

3.1 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**.

3.2 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

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)

3.3 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.

3.4 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.

3.5 Contact

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

privacy@settlday.com