SettlDay

SETTLEMENT READINESS PLATFORM

GET IT DONE

Contractual Pack

Version dc151e3
Generated 2026-04-14

SettlDay — A joint initiative by Kommalpha AG and amalics GmbH

settlday.com

Contents

1. Technical and Organisational Measures (TOMs)

Document ID	TOM-001
Classification	Public — Trust Center

1.1 Scope

This document describes the technical and organisational measures implemented by amalics GmbH ("Controller") to protect personal data processed in the SettlDay platform, in accordance with Art. 32 GDPR.

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).

This document serves as Annex 2 (Anlage: Technische und organisatorische Maßnahmen) to the Data Processing Agreement.

1.2 Access Control (Zutrittskontrolle)

Measures to prevent unauthorised physical access to data processing facilities:

- All infrastructure is hosted in professionally managed, certified data centres within the European Union (Frankfurt, Germany).
- Data centre facilities maintain ISO 27001 and SOC 2 certifications with physical security controls including biometric access, 24/7 surveillance, and multi-layer perimeter security.
- amalics GmbH does not operate on-premises servers. No personal data is stored on local devices or removable media.
- Administrative access to cloud infrastructure is restricted to authorised personnel using encrypted connections and multi-factor authentication.

1.3 System Access Control (Zugangskontrolle)

Measures to prevent unauthorised use of data processing systems:

- User authentication is managed through a self-hosted identity provider deployed on SettlDay's own EU infrastructure.

- Authentication uses industry-standard JWT-based token management with secure, time-limited sessions.
- Multi-factor authentication is available for all user accounts.
- Session management employs secure cookie handling with appropriate flags (HttpOnly, Secure, SameSite).
- Rate limiting is enforced on authentication endpoints to mitigate brute-force attacks.
- Password policies enforce minimum complexity requirements.
- Administrative access to infrastructure requires SSH key-based authentication with multi-factor verification.

1.4 Data Access Control (Zugriffskontrolle)

Measures to ensure that authorised users access only the data they are entitled to:

- Role-based access control (RBAC) enforces a hierarchical permission model (viewer, admin, owner).
- PostgreSQL Row-Level Security (RLS) provides database-level tenant isolation, ensuring that queries only return data belonging to the authenticated tenant.
- The principle of least privilege is enforced across all system components and administrative access.
- API authorisation checks are performed on every request, validating both authentication status and resource-level permissions.
- Access rights are reviewed and adjusted promptly upon role changes or offboarding.

1.5 Transfer Control (Weitergabekontrolle)

Measures to ensure data protection during electronic transmission and storage:

- All data in transit is protected by TLS 1.2 or higher. Unencrypted connections are rejected.
- All data at rest is encrypted using AES-256 encryption.
- All personal data is stored and processed exclusively in EU data centres (Frankfurt, Germany).
- AI inference is restricted to the EU region. Inference logging on the AI provider side is disabled to prevent data retention by third parties.
- No personal data is transferred to countries outside the EU/EEA without appropriate safeguards (Standard Contractual Clauses) in place.
- Email delivery uses TLS-encrypted SMTP connections via an EU-based provider.

1.6 Input Control (Eingabekontrolle)

Measures to ensure that it is possible to verify and establish who has entered, modified, or removed personal data:

- A comprehensive audit trail records all significant data operations, capturing timestamps, the acting user, the action performed, and the affected resource.

- All records maintain automatic tracking of creation and modification metadata (created_at, updated_at, created_by, updated_by).
- Structured application logging with automatic PII redaction ensures that log data itself does not become a privacy risk.
- Audit logs are tamper-resistant and retained in accordance with applicable data retention policies.

1.7 Job Control (Auftragskontrolle)

Measures to ensure that personal data processed on behalf of clients is processed strictly in accordance with instructions:

- Data processing is performed strictly in accordance with the Data Processing Agreement and the client's documented instructions.
- Sub-processor agreements are in place with all third parties involved in data processing (see Sub-Processor Register in the Vendor Due Diligence Pack at the SettlDay Trust Center).
- No client data is used for purposes beyond service delivery. In particular, no client data is used for training AI models.
- Employees and contractors with access to personal data are bound by confidentiality obligations.
- Regular reviews ensure continued compliance with contractual and regulatory requirements.

1.8 Availability Control (Verfügbarkeitskontrolle)

Measures to ensure that personal data is protected against accidental destruction or loss:

- Automated database backups with point-in-time recovery capability are maintained by the managed database provider.
- The application runs on a container orchestration platform with automatic restart, health monitoring, and self-healing capabilities.
- Documented incident response playbooks define roles, escalation paths, and communication procedures.
- A business continuity and disaster recovery plan is maintained and reviewed periodically.
- Infrastructure monitoring provides real-time alerting on system health and anomalies.

1.9 Separation Control (Trennungskontrolle)

Measures to ensure that data collected for different purposes is processed separately:

- Multi-tenant architecture enforces strict data separation at the database level using PostgreSQL Row-Level Security.
- Each organisation's data is logically isolated; cross-tenant data access is prevented by database-enforced policies, not merely application logic.
- Production and test environments are fully separated. No production data is used in testing.

- Assessment data is logically separated per organisation, ensuring that no client can access another client's assessments, reports, or configurations.

1.10 AI-Specific Measures

Additional measures specific to the use of artificial intelligence in the SettlDay platform:

- A multi-layer data minimisation pipeline processes all data before it reaches the AI provider:
  - **PII detection and replacement**: Named entity recognition identifies and replaces personal data with neutral placeholders before transmission.
  - **Firm name exclusion**: Organisation names are systematically removed from all data sent to the AI provider.
  - **Document summarisation**: Uploaded documents are summarised on SettlDay's own servers before any content is forwarded, minimising the data shared with the AI provider.
- The AI provider (accessed via AWS Bedrock in the EU region) retains zero client data. Inference logging is disabled at the provider level.
- AI outputs are advisory only. No automated decisions with legal effect are made by the system. All AI-generated content is clearly labelled and subject to human review.
- No client data is used for AI model training, fine-tuning, or improvement by any party.

1.11 Review and Updates

These measures are reviewed at least annually and updated to reflect changes in the threat landscape, regulatory requirements, or system architecture. The current version is always available at the SettlDay Trust Center.

1.12 Contact

amalics GmbH Simrockstr. 23, 80997 München, Germany

privacy@settlday.com

2. Data Processing Agreement

Document ID	DPA-CUST-001
Version	1.0
Date	2026-03-22
Classification	Contractual

2.1 PARTIES

1. Data Controller ("Controller"):

Field	Detail
Company Name	[CUSTOMER_NAME]
Registered Address	[CUSTOMER_ADDRESS]
Registration Number	[CUSTOMER_REGISTRATION_NUMBER]
Contact Person	[CUSTOMER_CONTACT_NAME]
Contact Email	[CUSTOMER_CONTACT_EMAIL]

2. Data Processor ("Processor"):

Field	Detail
Company Name	amalics GmbH, trading as SettlDay
Registered Address	Simrockstr. 23, 80997 Munchen, Germany
Registration Number	HRB 264611, Amtsgericht Munchen
Contact Person	Data Protection Contact
Contact Email	privacy@settlday.com

The Controller and the Processor are each a "Party" and together the "Parties."

This Data Processing Agreement ("DPA") forms part of and supplements the service agreement between the Parties for the provision of the SettlDay platform ("Service Agreement"). In the event of any conflict

between this DPA and the Service Agreement, this DPA shall prevail with respect to the processing of Personal Data.

2.2 DEFINITIONS

1.1. **"Applicable Data Protection Law"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, "GDPR"), and any national implementing legislation, as applicable to the processing of Personal Data under this DPA.

1.2. **"Controller"** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, as identified above.

1.3. **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.

1.4. **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.

1.5. **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed, as defined in Article 4(12) GDPR.

1.6. **"Processing"** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, as defined in Article 4(2) GDPR.

1.7. **"Processor"** means a natural or legal person which processes Personal Data on behalf of the Controller, as identified above.

1.8. **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

1.9. **"Supervisory Authority"** means an independent public authority established by an EU Member State pursuant to Article 51 GDPR.

1.10. **"Technical and Organisational Measures"** or **"TOMs"** means the security measures described in Annex II to this DPA.

2.3 SUBJECT MATTER AND DURATION

2.1. **Subject matter.** This DPA governs the processing of Personal Data by the Processor on behalf of the Controller in connection with the provision of the SettlDay T+1 Settlement Readiness Assessment Platform under the Service Agreement.

2.2. **Duration.** This DPA shall remain in effect for the duration of the Service Agreement and shall automatically terminate upon the termination or expiry of the Service Agreement, subject to Section 12 (Obligations on Termination).

2.3. **Governing law.** This DPA shall be governed by and construed in accordance with the laws of the Federal Republic of Germany, without regard to its conflict of laws provisions. The courts of Munich, Germany shall have exclusive jurisdiction over any disputes arising from this DPA.

2.4 NATURE AND PURPOSE OF PROCESSING

3.1. The Processor processes Personal Data solely for the purpose of providing the services described in the Service Agreement, which include:

(a) **Account management** – Creation and administration of user accounts, authentication, and role-based access control for the Controller's authorised users.

(b) **Assessment data collection** – Collection and storage of assessment responses relating to the Controller's T+1 settlement readiness, including firm profile data, maturity scores, and operational metrics.

(c) **AI-powered report generation** – Generation of personalised T+1 settlement readiness reports using large language models (LLMs), with pseudonymised and PII-scrubbed data transmitted to the AI inference provider (see Section 10, AI Processing Addendum).

(d) **Document analysis** – Extraction and summarisation of relevant operational information from documents uploaded by the Controller's users, for the purpose of personalising assessment reports.

(e) **Email delivery** – Transmission of transactional emails (account notifications, report delivery, assessment results) to the Controller's users.

(f) **Payment processing** – Processing of subscription payments and billing information for the Controller's account.

3.2. The Processor shall not process Personal Data for any purpose other than those specified in this Section 3, unless required to do so by EU or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.5 TYPES OF PERSONAL DATA

4.1. The following categories of Personal Data are processed under this DPA:

Category	Data Elements
Professional identity	First name, last name, business email address
Professional role	Job title, department

Category	Data Elements
Firm profile	Firm type, firm size, jurisdictions of operation
Assessment data	Maturity scores per category, operational KPIs (fail rates, STP rates), free-text comments
Account data	User role, login timestamps, session metadata
Payment data	Managed by Stripe; card details never touch Processor's servers (PCI DSS)

4.2. No special categories of Personal Data within the meaning of Article 9 GDPR are processed under this DPA. The Processor is not designed or intended to process special category data, and the Controller shall not submit such data to the platform.

2.6 CATEGORIES OF DATA SUBJECTS

5.1. The Personal Data processed under this DPA relates to the following categories of Data Subjects:

(a) **Employees and authorised representatives of the Controller** who use the SettlDay platform in their professional capacity (compliance officers, analysts, operations staff, management).

(b) **Third parties incidentally referenced** in documents uploaded by the Controller's users (names or contact details appearing in operational documents). Such data is processed only temporarily for document analysis and is subject to PII scrubbing controls described in Section 10.

2.7 OBLIGATIONS OF THE CONTROLLER

6.1. The Controller warrants that:

(a) It has determined the lawful basis for each processing activity under this DPA and can demonstrate compliance with Article 6 GDPR.

(b) It has provided appropriate privacy notices to Data Subjects whose Personal Data is submitted to the platform, informing them of the processing described in this DPA.

(c) It has obtained any necessary consents from Data Subjects, where consent is the lawful basis for processing.

(d) It shall not submit special categories of Personal Data (Article 9 GDPR) to the platform unless expressly agreed in writing with the Processor.

(e) It shall promptly notify the Processor of any changes to its processing instructions or any circumstances that may affect the Processor's ability to comply with this DPA.

2.8 OBLIGATIONS OF THE PROCESSOR

In accordance with Article 28(3) GDPR, the Processor shall:

2.8.1 Documented Instructions (Art. 28(3)(a))

(a) Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by EU or Member State law. The Service Agreement, this DPA, and the Controller's configuration of the platform constitute the Controller's documented instructions. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Applicable Data Protection Law.

2.8.2 Confidentiality (Art. 28(3)(b))

(b) Ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Personal Data is limited to those Processor personnel who require it to perform the services under the Service Agreement.

2.8.3 Security Measures (Art. 28(3)(c))

(c) Implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. The specific measures are described in **Annex II** (Technical and Organisational Measures) to this DPA. These measures include, but are not limited to:

- Encryption of Personal Data in transit (TLS 1.3) and at rest (AES-256)
- Tenant isolation via PostgreSQL Row-Level Security and application-level access controls
- Role-based access control with least-privilege enforcement
- Automated data retention and purging mechanisms
- PII detection and scrubbing before AI processing
- Comprehensive audit trail on all data operations

2.8.4 Sub-processing (Art. 28(3)(d))

(d) Not engage another processor (Sub-processor) without prior specific or general written authorisation of the Controller, in accordance with Section 8 of this DPA.

2.8.5 Data Subject Rights (Art. 28(3)(e))

(e) Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR (Articles 15 to 22).

The Processor provides the following mechanisms to support Data Subject rights:

- **Right of access (Art. 15):** Self-service data export functionality within the platform; DSAR access request endpoint.
- **Right to rectification (Art. 16):** Self-service profile editing within the platform; DSAR rectification request endpoint.
- **Right to erasure (Art. 17):** Self-service account deletion; DSAR erasure request endpoint that anonymises all Personal Data.
- **Right to restriction of processing (Art. 18):** Account suspension capability.
- **Right to data portability (Art. 20):** Self-service structured JSON data export.

The Processor shall promptly notify the Controller if it receives a request directly from a Data Subject and shall not respond to such request except on the Controller's documented instructions, unless required by Applicable Data Protection Law.

2.8.6 Assistance with Security Obligations (Art. 28(3)(f))

(f) Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor. This includes:

- **Article 32 (Security of processing):** Maintaining the Technical and Organisational Measures described in Annex II and notifying the Controller of any material changes.
- **Article 33 (Notification of a Personal Data Breach to the supervisory authority):** Notifying the Controller without undue delay after becoming aware of a Personal Data Breach (see Section 9).
- **Article 34 (Communication of a Personal Data Breach to the Data Subject):** Providing the Controller with sufficient information to enable the Controller to meet its obligations to inform Data Subjects.
- **Article 35 (Data Protection Impact Assessment):** Providing the Controller with information reasonably necessary to conduct a DPIA where required.
- **Article 36 (Prior consultation):** Providing the Controller with reasonable assistance in the event of prior consultation with a Supervisory Authority.

2.8.7 Deletion or Return of Data (Art. 28(3)(g))

(g) At the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless EU or Member State law requires storage of the Personal Data. The obligations under this clause are detailed in Section 12 (Obligations on Termination).

2.8.8 Audit Rights (Art. 28(3)(h); MaRisk AT 9.6; DORA Art. 30)

(h) Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, MaRisk AT 9, and DORA Art. 30, and allow for and

contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

- The Controller may conduct audits no more than once per calendar year, upon thirty (30) days' prior written notice to the Processor.
- Audits shall be conducted during normal business hours and shall not unreasonably interfere with the Processor's business operations.
- The Controller shall bear its own costs for any audit. If the audit requires the Processor to dedicate resources beyond a reasonable level, the Parties shall agree on fair compensation in advance.
- The auditor shall be bound by appropriate confidentiality obligations.
- Where the Processor has obtained relevant certifications or audit reports (e.g., SOC 2 Type II), the Processor may provide these to the Controller as evidence of compliance in lieu of an on-site inspection, provided the Controller may still exercise its audit right where the certification or report does not address specific concerns raised in writing.

Competent Authority Access. The Processor shall grant the Controller's competent supervisory authority (including BaFin, the European Supervisory Authorities, and any other authority with jurisdiction over the Controller) unrestricted rights of access, inspection, and audit of the Processor's premises, systems, and documentation relevant to the services provided under this DPA. The Processor shall cooperate fully with such authorities in the exercise of their supervisory functions. This obligation extends to the Processor's Sub-processors to the extent required by applicable law or regulation.

Audit Pooling. Where multiple Controllers wish to exercise their audit rights concurrently or where the Controller participates in a pooled audit arrangement (e.g., through an industry association or shared audit initiative), the Processor shall accommodate such pooled audits. The Processor shall designate a point of contact for coordinating pooled audit requests and shall use reasonable efforts to schedule pooled audits efficiently to minimise disruption to all parties. The costs of a pooled audit shall be shared among the participating Controllers as agreed between them.

2.9 SUB-PROCESSORS

2.9.1 Authorised Sub-processors

The Controller provides general authorisation for the Processor to engage the Sub-processors listed in **Annex I** (Authorised Sub-processors) to this DPA. The Processor shall ensure that each Sub-processor is bound by data protection obligations no less protective than those set out in this DPA, in accordance with Article 28(4) GDPR.

2.9.2 Changes to Sub-processors

(a) The Processor shall notify the Controller in writing at least thirty (30) days before engaging any new Sub-processor or replacing an existing Sub-processor ("Sub-processor Change Notice"). The notification shall include the identity of the proposed Sub-processor, its location, and the nature of the processing to be performed.

(b) The Controller may object to the engagement of a new Sub-processor on reasonable grounds relating to data protection by notifying the Processor in writing within fifteen (15) days of receiving the Sub-processor Change Notice.

(c) Where the Controller raises a reasonable objection, the Processor shall use commercially reasonable efforts to make available to the Controller a change in the services or recommend a commercially reasonable change to the Controller's configuration or use of the services to avoid processing of Personal Data by the objected-to Sub-processor, without unreasonably burdening the Controller.

(d) If the Processor is unable to accommodate the Controller's objection and the Controller maintains its objection, either Party may terminate the affected portion of the Service Agreement by providing thirty (30) days' written notice, without penalty to either Party.

2.9.3 Liability for Sub-processors

The Processor shall remain fully liable to the Controller for the performance of each Sub-processor's obligations under the sub-processing agreement. Where a Sub-processor fails to fulfil its data protection obligations, the Processor shall remain liable to the Controller for the acts and omissions of the Sub-processor as if they were the acts and omissions of the Processor.

2.10 PERSONAL DATA BREACH NOTIFICATION

9.1. The Processor shall notify the Controller without undue delay, and in any event within **forty-eight (48) hours**, after becoming aware of a Personal Data Breach affecting the Controller's Personal Data.

9.2. The notification shall include, to the extent reasonably available:

(a) A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned.

(b) The name and contact details of the Processor's data protection contact from whom further information can be obtained.

(c) A description of the likely consequences of the Personal Data Breach.

(d) A description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3. Where it is not possible to provide the information at the same time as the initial notification, the information may be provided in phases without undue further delay.

9.4. The Processor shall cooperate with and assist the Controller in investigating and remediating the Personal Data Breach and in meeting the Controller's obligations under Articles 33 and 34 GDPR.

9.5. The Processor shall document all Personal Data Breaches, including the facts relating to the breach, its effects, and the remedial action taken, and shall make this documentation available to the Controller upon request.

2.11 AI PROCESSING ADDENDUM

This section sets out specific provisions governing the use of artificial intelligence (large language models) within the SettlDay platform. These provisions supplement the general obligations of the Processor under this DPA.

2.11.1 AI Processing Architecture

(a) The Processor uses large language models ("LLMs") hosted on **AWS Bedrock** within EU regions (Ireland, Frankfurt, Paris, Stockholm) to generate personalised T+1 settlement readiness reports based on the Controller's assessment data.

(b) The AI inference provider is **Amazon Web Services EMEA SARL** (Luxembourg). Anthropic, as the developer of the Claude model, does **not** receive, process, or store any Controller data. The Claude model runs on AWS-managed infrastructure within the EU. The processor relationship for AI inference is with AWS, not Anthropic.

2.11.2 No Training on Controller Data

(a) The Controller's Personal Data and assessment data are **never** used to train, fine-tune, improve, or evaluate any AI or machine learning model.

(b) AWS Bedrock's terms of service contractually prohibit the use of customer inputs and outputs for model training or improvement.

(c) The Processor does not operate or contribute to any model training pipeline using Controller data.

2.11.3 Zero Retention by AI Inference Provider

(a) **Inference logging is disabled** on the Processor's AWS Bedrock configuration. This means that neither the inputs (prompts) nor the outputs (completions) sent to and received from the LLM are retained by AWS after inference.

(b) The AI inference provider processes data in memory for the duration of the inference request only. No data is written to persistent storage by the AI inference provider.

2.11.4 PII Scrubbing and Data Minimisation

(a) Before any data is transmitted to the AI inference provider, the Processor applies the following data minimisation controls:

- **Firm name exclusion:** The Controller's firm name is stripped from all data sent to the LLM. The firm name is re-inserted into the generated report on the Processor's EU servers after inference, and is never transmitted to the AI provider.
- **PII detection and replacement:** A natural language processing pipeline (spaCy Named Entity Recognition) scans all free-text fields and document excerpts for personal identifiers (names, email addresses, phone numbers) and replaces them with anonymised placeholders before transmission.
- **Document summarisation:** Documents uploaded by the Controller's users are summarised on the Processor's EU servers. Only structured excerpts – not raw document content – are forwarded to the AI inference provider. Original files are deleted immediately after text extraction.

(b) As a result of these controls, the data transmitted to the AI inference provider is limited to:

- Firm type (e.g., asset manager, broker-dealer)
- Firm size category
- Jurisdictions of operation
- Anonymised maturity scores and operational metrics
- PII-scrubbed free-text excerpts

2.11.5 No Automated Decision-Making with Legal Effect

(a) The AI-generated reports and assessment scores produced by the platform are **advisory only**. They do not constitute automated decision-making producing legal effects or similarly significantly affecting Data Subjects within the meaning of Article 22 GDPR.

(b) All AI-generated content is intended for review and interpretation by qualified professionals at the Controller's organisation.

2.12 INTERNATIONAL DATA TRANSFERS

11.1. **EU-only processing.** All Personal Data processed under this DPA is stored and processed within the European Economic Area (EEA). The Processor's infrastructure, databases, and AI inference services operate exclusively from EU data centres.

11.2. **No transfers outside the EEA.** The Processor does not transfer Personal Data outside the EEA in the course of providing the services under the Service Agreement. The current Sub-processor architecture (Annex I) is designed to ensure all processing remains within EU jurisdiction.

11.3. **Stripe (payments).** Payment data is processed by Stripe, Inc. (US) in accordance with Stripe's Data Processing Agreement, which includes EU Standard Contractual Clauses (SCCs) for any transfers

outside the EEA. Card details are collected directly by Stripe via Stripe.js and never touch the Processor's servers.

11.4. **Future changes.** If the Processor anticipates a need to transfer Personal Data outside the EEA in the future, it shall:

(a) Notify the Controller in writing at least thirty (30) days in advance.

(b) Ensure that appropriate safeguards are in place in accordance with Chapter V of the GDPR (e.g., Standard Contractual Clauses, adequacy decisions).

(c) Provide the Controller with the opportunity to object in accordance with Section 8.2 of this DPA.

2.13 OBLIGATIONS ON TERMINATION

12.1. Upon termination or expiry of the Service Agreement, the Controller may request, within thirty (30) days of termination:

(a) **Return of data:** The Processor shall provide the Controller with a complete export of all Personal Data in a structured, commonly used, and machine-readable format (JSON).

(b) **Deletion of data:** The Processor shall delete all Personal Data from its systems, including any copies held by Sub-processors, within thirty (30) days of the Controller's deletion request or, if no request is made, within ninety (90) days of termination.

12.2. The Processor shall provide written confirmation of deletion to the Controller upon request.

12.3. The Processor may retain Personal Data to the extent required by EU or Member State law, provided that the Processor:

(a) Processes such retained data only for the purpose required by law.

(b) Ensures appropriate confidentiality and security measures remain in place.

(c) Informs the Controller of the legal requirement and the categories of data retained.

12.4. Backup copies containing Personal Data shall be purged in accordance with the Processor's standard backup rotation schedule, which does not exceed ninety (90) days.

2.14 LIABILITY

13.1. Each Party's liability under this DPA shall be subject to the limitations and exclusions of liability set out in the Service Agreement, except that neither Party may limit its liability for:

(a) Damage caused by processing that does not comply with the obligations of the GDPR specifically directed to processors (Article 82(2) GDPR).

(b) Damage caused by processing outside or contrary to the lawful instructions of the Controller, where the Processor has acted outside or contrary to the Controller's documented instructions.

13.2. Where the Processor is held liable under Article 82(2) GDPR for damage caused by processing in violation of GDPR obligations specifically directed to processors, or where the Processor has acted outside or contrary to the Controller's lawful instructions, the Processor shall be liable for the damage caused by the processing to the extent of its responsibility.

13.3. Where the Controller is held liable under Article 82(2) GDPR for damage caused by processing, and the Processor has complied with its obligations under this DPA and GDPR, the Controller shall indemnify the Processor for any liability, costs, and damages incurred.

13.4. The Parties shall cooperate in good faith in addressing any claims from Data Subjects or Supervisory Authorities arising from the processing of Personal Data under this DPA.

2.15 GENERAL PROVISIONS

14.1. **Amendments.** This DPA may be amended only by written agreement signed by both Parties.

14.2. **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The Parties shall negotiate in good faith to replace the invalid provision with a valid provision that achieves the original intent.

14.3. **Entire agreement.** This DPA, together with its Annexes and the Service Agreement, constitutes the entire agreement between the Parties regarding the processing of Personal Data and supersedes all prior or contemporaneous agreements, representations, and understandings relating to such processing.

14.4. **Notices.** All notices under this DPA shall be in writing and sent to the contact addresses specified in the Parties section above, or to such other address as a Party may designate in writing.

14.5. **No waiver.** A failure or delay by either Party in exercising any right under this DPA shall not constitute a waiver of that right.

2.16 SIGNATURES

This DPA is entered into and becomes binding upon the Parties as of the date of the last signature below ("Effective Date").

For the Controller:

Field	Detail
Name	_____

Field	Detail
Title	_____
Company	[CUSTOMER_NAME]
Date	_____
Signature	_____

For the Processor:

Field	Detail
Name	_____
Title	_____
Company	amalics GmbH (trading as SettlDay)
Date	_____
Signature	_____

2.17 ANNEX I – AUTHORISED SUB-PROCESSORS

The following Sub-processors are authorised by the Controller as of the Effective Date of this DPA:

Sub-processor	Legal Entity	Location	Processing Activity	Personal Data Involved	DPA Mechanism
DigitalOcean	DigitalOcean, LLC	EU data centres (Amsterdam, Frankfurt)	Cloud infrastructure hosting – compute, storage, managed PostgreSQL databases	All platform data (encrypted at rest and in transit)	DigitalOcean Data Processing Agreement (incorporated in Terms of Service)
Amazon Web Services (Bedrock)	Amazon Web Services EMEA SARL	EU regions (Ireland, Frankfurt, Paris, Stockholm)	AI inference for report generation – pseudonymised assessment data processed in memory; no	Firm type, firm size, jurisdictions, anonymised scores, PII-scrubbed free-text	AWS GDPR Data Processing Addendum + EU SCCs (AWS Customer Agreement)

Sub-processor	Legal Entity	Location	Processing Activity	Personal Data Involved	DPA Mechanism
			retention after inference	excerpts. No firm name, no user identity.	
IONOS	IONOS SE	Germany	Transactional email delivery – account notifications, report delivery	Email addresses (in transit only)	IONOS Data Processing Agreement (incorporated in business contract)
Stripe	Stripe, Inc.	United States (with EU SCCs)	Payment processing – subscription billing, invoicing	Payment card details (collected via Stripe.js, never stored on Processor servers), billing email	Stripe Data Processing Agreement (signed) + EU SCCs
FusionAuth (self-hosted)	N/A – self-hosted on Processor's EU infrastructure	EU (DigitalOcean infrastructure)	User authentication and identity management	User profiles, hashed credentials, login history, session tokens	N/A – no data leaves Processor's control. FusionAuth is operated by the Processor on its own EU infrastructure.
Matomo (self-hosted)	N/A – self-hosted on Processor's EU infrastructure	EU (DigitalOcean infrastructure)	Anonymised product analytics (cookieless mode)	Anonymised usage metrics only – no individually identifiable Personal Data	N/A – no data leaves Processor's control. Matomo is operated by the Processor in cookieless mode with k-anonymity enforcement.

Note on Anthropic: Anthropic, PBC does not appear in this Sub-processor list because it is not a Sub-processor. Claude models are invoked via AWS Bedrock on AWS-managed infrastructure within the EU. Anthropic does not receive, process, or store any Controller data.

2.18 ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES (Art. 32 GDPR)

The Processor implements the following technical and organisational measures to protect Personal Data:

2.18.1 Encryption

Measure	Detail
Data in transit	TLS 1.3 enforced for all client-server and service-to-service communication via ingress-nginx with cert-manager (Let's Encrypt certificates)
Data at rest	AES-256 encryption on all database storage and object storage (DigitalOcean managed volumes)
Backups	Encrypted daily backups with point-in-time recovery; restoration tested periodically

2.18.2 Access Control

Measure	Detail
Authentication	JWT-based authentication via self-hosted FusionAuth; support for multi-factor authentication
Authorisation	Role-Based Access Control (RBAC) with role hierarchy (viewer, admin, owner); least-privilege principle enforced
Tenant isolation	PostgreSQL Row-Level Security (RLS) policies enforce strict tenant boundaries; application-level organisation_id filtering on all queries
Credential management	Passwords hashed with bcrypt/argon2; no plaintext credentials stored
Session management	Short-lived JWT tokens; server-side session invalidation on logout
Internal access	Engineering access to production data limited, logged, and subject to periodic review; no standing access to Personal Data

2.18.3 Data Minimisation

Measure	Detail
Firm name exclusion	Controller's firm name is never transmitted to the AI inference provider; re-inserted post-processing on Processor's EU servers
PII scrubbing	

Measure	Detail
	spaCy Named Entity Recognition pipeline detects and replaces personal identifiers with anonymised placeholders before any AI processing
Document handling	Uploaded documents are never persisted to long-term storage; only summarised excerpts are retained for the assessment session; originals deleted immediately after text extraction
Analytics anonymisation	k-anonymity threshold (minimum 10 sessions per cohort) enforced before any aggregate data is exposed; Matomo operates in cookieless mode

2.18.4 Pseudonymisation

Measure	Detail
AI pipeline	Assessment data forwarded to the LLM uses firm type/size/jurisdiction identifiers without firm name or user identity
Analytics	User identifiers replaced with session-scoped pseudonyms; Matomo user IDs are SHA-256 hashed before transmission

2.18.5 Input Validation and Application Security

Measure	Detail
Input validation	Pydantic v2 schemas with strict type checking, field length limits, regex patterns, and enum validation
Rate limiting	Global middleware rate limiting plus per-endpoint rate limits on PII-sensitive endpoints
Security headers	HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy
Vulnerability scanning	Trivy vulnerability scanning on container images in CI/CD pipeline
Prompt injection defence	System prompt hardening and output validation for AI-generated content

2.18.6 Integrity and Availability

Measure	Detail
Database backups	Daily encrypted backups with point-in-time recovery on DigitalOcean Managed Databases
High availability	Managed PostgreSQL with automated failover

Measure	Detail
Monitoring	Uptime monitoring and alerting; structured logging with error tracking
Business continuity	Business Continuity and Disaster Recovery plan documented and maintained

2.18.7 Data Retention and Deletion

Measure	Detail
Automated retention	Daily automated task anonymises and purges Personal Data that has exceeded its defined retention period
Soft deletes	All client data uses soft deletion with PII anonymisation at the point of deletion
Hard purge	Soft-deleted records are permanently removed after a defined grace period
Backup rotation	Backup snapshots retained for a maximum of 90 days

2.18.8 Audit and Logging

Measure	Detail
Audit trail	All data records carry creation and modification timestamps with actor identification
PII scrubbing in logs	Structured logging with 35+ PII-key patterns automatically redacted from all log output
DSAR audit records	All Data Subject access requests are logged with request identifiers and types (no PII in log entries)

2.18.9 Incident Response

Measure	Detail
Breach detection	Automated alerting on anomalous access patterns and error rates
Incident response playbooks	Documented playbooks covering service outage, brute force attacks, account compromise, data breach, and supply chain incidents
Notification timeline	Personal Data Breach notification to Controller within 48 hours of awareness (see Section 9 of this DPA)

2.18.10 Personnel Measures

Measure	Detail
Confidentiality	All personnel with access to Personal Data are bound by contractual confidentiality obligations
Training	Data protection awareness training for all staff handling Personal Data
Access reviews	Periodic review of access privileges to ensure continued necessity

---

2.19 ANNEX III – CONTROLLER'S PROCESSING INSTRUCTIONS

The Controller instructs the Processor to process Personal Data as follows:

1. **Provision of services.** Process Personal Data to the extent necessary to provide the services described in the Service Agreement, including account management, assessment data collection, AI report generation, document analysis, email delivery, and payment processing.
2. **Data Subject rights.** Process Personal Data as necessary to assist the Controller in responding to Data Subject requests under Chapter III GDPR.
3. **Security.** Process Personal Data as necessary to detect and prevent security incidents, fraud, and abuse.
4. **Legal compliance.** Process Personal Data as necessary to comply with applicable EU or Member State law.
5. **Controller instructions.** Process Personal Data in accordance with any additional documented instructions provided by the Controller from time to time, provided such instructions are consistent with the Service Agreement and Applicable Data Protection Law.

Any processing beyond these instructions requires the prior written agreement of both Parties.

End of Data Processing Agreement