TenderMind

12 JULY 2026

Contract Codification

PROJECT NAME

Demo Sample

AUTOMATE WHAT CAN BE REPEATED.

GUIDE WHAT MATTERS.

Table of Contents

1. Contracting Parties and Agreement Structure

1.1 Codified Summary

The agreement is entered into between **Asteron Meridian Group Ltd.**, acting as the customer, and **Nexora Contract Systems Ltd.**, acting as the supplier.

The Customer is described as a diversified corporate group with centralised procurement, legal, finance, and operational functions. The Supplier is described as a provider of enterprise software, artificial intelligence-assisted document processing, and managed procurement support services.

The agreement consists of the main contractual document and a series of schedules. In the event of inconsistency, the main body of the agreement takes precedence unless a schedule expressly states that it overrides a specific provision.

1.2 Contracting Parties

Role	Legal Entity	Registered Address	Contractual Function
Customer	Asteron Meridian Group Ltd.	18 Meridian Square, Novaris, Norland	Purchaser and authorised user of the services
Supplier	Nexora Contract Systems Ltd.	42 Innovation Harbour, Bellmont, Norland	Technology provider and managed service operator

1.3 Agreement Documents

The agreement includes the following documents:

1. Main Managed Procurement Intelligence Services Agreement.
2. Schedule 1 – Service Description.
3. Schedule 2 – Implementation Plan.
4. Schedule 3 – Fees and Payment Schedule.
5. Schedule 4 – Service-Level Agreement.
6. Schedule 5 – Data Processing Terms.
7. Schedule 6 – Information Security Requirements.
8. Schedule 7 – Exit and Transition Plan.

1.4 Order of Precedence

The following order of precedence applies:

1. Signed amendments and change orders.
2. Main agreement.
3. Data Processing Terms.
4. Information Security Requirements.
5. Service-Level Agreement.
6. Service Description.
7. Implementation Plan.
8. Commercial proposal and supporting documentation.

Any purchase order issued by the Customer is treated as an administrative document only. Additional or conflicting terms included in a purchase order do not amend the agreement unless expressly accepted in writing by both parties.

1.5 Authorised Representatives

Each party must appoint:

- One executive sponsor.
- One contract manager.
- One operational contact.
- One information security contact.
- One finance and invoicing contact.

Changes to authorised representatives must be communicated in writing within five business days.

1.6 Key Obligations

Customer

- Ensure that its representatives have authority to provide instructions and approvals.
- Notify the Supplier of changes in ownership, legal status, or authorised contacts.
- Avoid issuing instructions through unauthorised personnel.

Supplier

- Accept contractual instructions only from authorised Customer representatives.
- Maintain a current stakeholder and escalation register.
- Notify the Customer before replacing key Supplier personnel.

1.7 Identified Contract Risk

The agreement permits operational instructions to be issued by designated representatives but does not provide a detailed approval matrix for instructions that may increase cost. This creates a risk that operational requests could be treated as chargeable changes without prior executive approval.

Recommended Control	Define financial approval thresholds and authorised approvers within the governance schedule.

2. Purpose, Scope, and Contract Objectives

2.1 Codified Summary

The purpose of the agreement is to deploy and operate a managed digital platform that assists the Customer in analysing procurement documents, evaluating supplier submissions, monitoring contractual obligations, and generating structured reports.

The Supplier must provide both the underlying software platform and the professional services required to configure, implement, support, and maintain the solution.

2.2 Contract Objectives

The principal objectives are:

- Standardise the review of tenders, contracts, proposals, and supplier submissions.
- Reduce manual document review and administrative processing.
- Improve consistency and traceability in supplier evaluations.
- Produce structured outputs with references to source documents.
- Monitor obligations, deadlines, deliverables, and contractual risks.
- Support procurement, legal, finance, and operational teams.
- Maintain appropriate security, confidentiality, and data governance controls.

2.3 Included Services

The Supplier must provide:

Platform Services

- Secure user authentication.
- Role-based access control.
- Document upload and storage.
- Contract and tender document analysis.
- Extraction of clauses, obligations, dates, and deliverables.
- Supplier response evaluation.
- Configurable evaluation criteria.
- Structured reporting.
- Export to PDF, Word, Excel, and machine-readable formats.
- Dashboard and audit-trail functionality.

Implementation Services

- Requirements gathering.
- Solution configuration.
- User-role design.
- Workflow setup.
- Template configuration.
- Historical document migration.
- Testing support.
- User acceptance testing coordination.
- Administrator and end-user training.

Managed Services

- Platform monitoring.
- Incident management.
- Application support.
- Configuration assistance.
- Monthly service reporting.
- Quarterly service review meetings.
- Minor workflow adjustments within the agreed support allocation.

2.4 Excluded Services

Unless approved through change control, the following are excluded:

- Legal advice or legal interpretation.
- Final procurement award decisions.
- Independent financial audits.
- Custom integrations not listed in the implementation plan.
- Manual correction of poor-quality source documents exceeding the agreed processing threshold.
- Translation services.
- On-site support outside the agreed implementation workshops.
- Development of entirely new software modules.
- Long-term storage beyond the agreed retention period.

2.5 Geographic Scope

The platform may be used by authorised Customer entities located within the European Economic Area. Deployment outside the approved territory requires prior written approval and may be subject to additional security, data protection, tax, and licensing requirements.

2.6 User Scope

The agreement includes:

- Up to 150 named users.
- Up to 20 administrator users.
- Up to five Customer legal entities.
- Up to 50,000 processed document pages per contract year.

Additional users, entities, or document volumes may result in additional fees.

2.7 Output Limitation

The platform outputs are decision-support materials. They do not replace professional legal, financial, technical, or procurement judgment.

The Customer remains responsible for:

- Reviewing generated outputs.
- Confirming the accuracy of extracted information.
- Making final procurement or contractual decisions.
- Obtaining specialist advice where required.

2.8 Key Scope Risk

The distinction between “minor workflow adjustments” and “new software modules” is not objectively defined.

Recommended Control	Introduce measurable thresholds based on development effort, affected workflows, number of new data fields, and estimated implementation hours.

3. Definitions and Interpretation

3.1 Codified Summary

The agreement contains defined terms governing the interpretation of operational, technical, commercial, and legal provisions.

Defined terms apply throughout the agreement and all schedules unless the context requires otherwise.

3.2 Key Definitions

Term	Codified Definition
Authorised User	An employee, contractor, or representative approved by the Customer to access the Services
Business Day	Any day other than Saturday, Sunday, or a public holiday in Norland
Change Request	A documented request to amend the Services, Deliverables, fees, scope, or implementation plan
Customer Data	All information, documents, records, and content submitted to or processed through the Services
Deliverable	Any document, configuration, report, integration, template, or other output the Supplier must provide
Documentation	User guides, technical materials, training documents, and operating instructions
Incident	An event that causes or may cause interruption, degradation, loss, or unauthorised access
Personal Data	Information relating to an identified or identifiable natural person
Platform	The Supplier's hosted procurement intelligence software environment
Professional Services	Configuration, implementation, training, migration, integration, and advisory services
Services	The Platform Services, Professional Services, support, maintenance, and managed services
Service Level	A measurable performance commitment defined in the Service-Level Agreement
Supplier Personnel	Employees, consultants, subcontractors, and agents used by the Supplier
Customer Materials	Templates, policies, evaluation criteria, and content provided by the Customer
Acceptance Criteria	The documented requirements used to determine whether a Deliverable is accepted

3.3 Interpretation Rules

The agreement provides that:

- Headings do not affect interpretation.
- References to legislation include amendments and replacement legislation.
- Singular terms include the plural and vice versa.
- "Including" means "including without limitation."
- Written communication includes approved electronic communication.
- A requirement for consent means prior written consent.

- References to days mean calendar days unless stated otherwise.
- References to business days exclude weekends and public holidays.
- Obligations not to perform an action include obligations not to permit that action.
- Schedules form part of the agreement.

3.4 Conflict Between Definitions

Where a term is defined in both the main agreement and a schedule, the definition in the main agreement applies unless the schedule expressly states that its definition applies only to that schedule.

3.5 Materiality Threshold

The term “material” is used in several provisions but is not assigned a quantitative threshold. Materiality must therefore be assessed based on the circumstances, including:

- Financial impact.
- Operational disruption.
- Security implications.
- Regulatory impact.
- Duration.
- Effect on contractual objectives.

3.6 Identified Interpretation Risk

Terms such as “reasonable efforts,” “promptly,” “material degradation,” and “industry-standard security” are used without measurable criteria.

Recommended Control	Replace subjective terms with defined time limits, technical standards, and financial or operational thresholds wherever practicable.

4. Contract Term, Implementation, and Milestones

4.1 Codified Summary

The agreement begins on 15 March 2026 and continues for an initial period of 24 months.

Following the Initial Term, the agreement renews automatically for successive 12-month periods unless either party provides at least 90 days’ written notice before the end of the current term.

4.2 Contract Timeline

Milestone	Target Date	Responsible Party
Contract Effective Date	15 March 2026	Both Parties
Project Kick-off	Within 5 Business Days	Both Parties
Requirements Confirmation	Week 2	Customer and Supplier
Configuration Completion	Week 6	Supplier
Integration Testing	Week 8	Supplier

Milestone	Target Date	Responsible Party
User Acceptance Testing Start	Week 9	Customer
User Acceptance Testing Completion	Week 11	Customer
Production Go-Live	Week 12	Supplier
First Service Review	30 days after Go-Live	Both Parties
Initial Term Expiry	14 March 2028	Both Parties

4.3 Implementation Phases

Phase 1 – Mobilisation

The parties establish project governance, confirm key contacts, approve the project plan, and validate technical prerequisites.

Phase 2 – Discovery and Design

The Supplier conducts workshops to document:

- Existing procurement workflows.
- Contract review processes.
- User roles.
- Approval requirements.
- Required outputs.
- Reporting formats.
- Integration points.
- Data retention requirements.

Phase 3 – Configuration

The Supplier configures:

- User groups.
- Access permissions.
- Document categories.
- Codification templates.
- Evaluation criteria.
- Reporting structures.
- Notifications.
- Dashboards.

Phase 4 – Testing

The Supplier conducts internal testing before releasing the configured environment for Customer testing.

Testing includes:

- Functional testing.
- Permission testing.

- Document-processing testing.
- Output validation.
- Security testing.
- Integration testing.
- Performance testing.

Phase 5 – User Acceptance Testing

The Customer receives ten business days to perform user acceptance testing.

The Customer must document identified issues and classify each issue as:

- Critical.
- High.
- Medium.
- Low.
- Enhancement request.

Phase 6 – Go-Live

Go-Live occurs when:

- Critical defects have been resolved.
- High-severity defects have an agreed resolution plan.
- Required integrations are operational.
- Administrator training is complete.
- Production access has been approved.
- The Customer provides written Go-Live authorisation.

4.4 Delay Management

A party that becomes aware of a potential delay must notify the other party promptly and provide:

- The reason for the delay.
- The affected milestone.
- The expected duration.
- Proposed mitigation measures.
- Any required decision or action.

Supplier-caused delays do not automatically extend milestone dates. An extension requires an approved change to the implementation plan.

Customer-caused delays may result in:

- Revised implementation dates.
- Additional professional-service fees.
- Reallocation of Supplier personnel.
- Delayed Go-Live.

4.5 Renewal Mechanism

The Supplier must notify the Customer at least 120 days before the end of the Initial Term or any renewal term.

The renewal notice must include:

- Current fees.
- Proposed renewal fees.
- Service usage.
- Unresolved issues.
- Proposed service changes.
- Applicable notice deadline.

4.6 Milestone Risk

The agreement requires the Customer to complete acceptance testing within ten business days. Failure to respond may result in deemed acceptance.

Recommended Control	Require the Supplier to issue a formal acceptance reminder and grant an additional five-business-day cure period before deemed acceptance applies.

5. Supplier Obligations and Responsibilities

5.1 Codified Summary

The Supplier is responsible for providing the Services with reasonable skill, care, diligence, and professional competence.

The Supplier must ensure that the Platform remains operational, secure, properly maintained, and capable of delivering the functionality described in the agreement.

5.2 Core Supplier Obligations

The Supplier must:

- Provide the Services in accordance with the agreement.
- Allocate appropriately qualified personnel.
- Maintain sufficient technical and operational capacity.
- Comply with applicable laws.
- Follow the Customer's documented security requirements.
- Maintain project and service records.
- Provide accurate service reports.
- Cooperate with Customer audits.
- Notify the Customer of material risks and incidents.
- Maintain appropriate insurance coverage.

5.3 Personnel Obligations

Supplier Personnel must possess suitable:

- Technical qualifications.
- Platform knowledge.
- Procurement-process understanding.
- Security awareness.
- Data protection training.
- Communication skills.

The Supplier must perform background checks where legally permitted and appropriate to the individual's role.

Key Supplier Personnel may not be replaced without reasonable notice, except in cases of resignation, illness, misconduct, or circumstances outside the Supplier's control.

Replacement personnel must have equivalent or superior experience.

5.4 Subcontracting

The Supplier may use approved subcontractors but remains fully responsible for their actions and omissions.

The Supplier must:

- Maintain a current subcontractor register.
- Conduct due diligence before appointment.
- Impose equivalent confidentiality and security obligations.
- Obtain approval before appointing a subcontractor that will process Customer Personal Data.
- Notify the Customer of material subcontractor changes.

The Customer may object to a new subcontractor on reasonable data protection or information security grounds.

5.5 Compliance Obligations

The Supplier must comply with:

- Applicable data protection legislation.
- Anti-bribery and anti-corruption requirements.
- Sanctions and trade-control laws.
- Employment and labour laws.
- Tax obligations.
- Information security obligations.
- Software licensing requirements.
- Accessibility obligations applicable to the Services.

5.6 Documentation and Reporting

The Supplier must maintain and provide:

- Updated user documentation.

- Administrator guides.
- Release notes.
- Security documentation.
- Monthly service reports.
- Incident reports.
- Change logs.
- Training materials.
- Data-flow information.
- Audit records.

Monthly reports must include:

- Service availability.
- Incident volumes.
- Response and resolution performance.
- User activity.
- Document-processing volumes.
- Support requests.
- Planned changes.
- Security events.
- Open risks and actions.

5.7 Notification Obligations

The Supplier must notify the Customer of:

- Critical service incidents.
- Confirmed or suspected data breaches.
- Material security vulnerabilities.
- Planned service interruptions.
- Changes to hosting locations.
- Material subcontractor changes.
- Legal or regulatory requests involving Customer Data.
- Circumstances likely to delay a Deliverable.
- Events that may materially affect the Supplier's ability to perform.

5.8 Business Continuity

The Supplier must maintain:

- A business continuity plan.
- A disaster recovery plan.
- Backup procedures.
- Recovery testing.
- Incident escalation procedures.
- Alternative staffing arrangements.

Business continuity and disaster recovery plans must be tested at least annually.

5.9 Supplier Dependency Risk

The agreement requires the Supplier to maintain sufficient capacity but does not specify minimum staffing levels or named backup personnel.

Recommended Control	Include a resourcing plan for critical roles and minimum continuity requirements for key operational functions.

6. Customer Obligations and Dependencies

6.1 Codified Summary

The Customer must provide the information, access, decisions, personnel, and technical cooperation reasonably required for the Supplier to perform the Services.

Supplier performance is dependent on timely Customer participation.

6.2 Customer Responsibilities

The Customer must:

- Provide accurate and complete requirements.
- Appoint authorised project representatives.
- Make personnel available for workshops and testing.
- Provide access to required systems.
- Supply Customer Materials in agreed formats.
- Review Deliverables within the specified timeframes.
- Maintain valid user information.
- Ensure lawful use of the Services.
- Pay undisputed invoices.
- Notify the Supplier of security incidents affecting the Platform.
- Maintain its own network, devices, and internet connectivity.

6.3 Customer Data Quality

The Customer is responsible for the quality and legality of Customer Data.

The Customer must ensure that:

- It has the right to upload and process the data.
- Documents do not contain unnecessary Personal Data.
- Files are not knowingly infected with malicious code.
- Information provided for analysis is accurate and complete.
- Data classifications are correctly applied.
- Retention instructions are communicated.

The Supplier is not responsible for errors caused by incomplete, inaccurate, corrupted, illegible, or misleading source documents.

6.4 Access and Credentials

The Customer must:

- Prevent unauthorised account sharing.
- Maintain appropriate password controls.
- Deactivate accounts promptly.
- Review administrator permissions regularly.
- Notify the Supplier of suspected credential compromise.
- Ensure users comply with acceptable-use requirements.

6.5 Review and Approval Obligations

The Customer must review:

- Requirements documentation.
- Configuration decisions.
- Test results.
- Deliverables.
- Change requests.
- Service reports.
- Security notifications.
- Renewal proposals.

Where the Customer does not respond within an agreed review period, the Supplier may issue a written reminder.

Continued failure to respond may affect project milestones but does not automatically authorise additional fees unless the Supplier identifies the financial impact in advance.

6.6 Prohibited Use

The Customer must not:

- Use the Platform for unlawful purposes.
- Attempt to access another customer's environment.
- Reverse engineer restricted Supplier technology.
- Introduce malware.
- Bypass security controls.
- Conduct unauthorised penetration testing.
- Resell the Services.
- Use automated outputs as the sole basis for legally significant decisions without appropriate human review.

6.7 Customer Dependency Risk

Several Supplier obligations depend on timely Customer approvals, but the agreement does not include a consolidated dependency schedule.

Recommended Control	Maintain a formal dependency register identifying each Customer action, owner, due date, and impact of delay.

7. Deliverables, Acceptance, and Change Control

7.1 Codified Summary

The Supplier must provide defined implementation, technical, training, and operational Deliverables.

Deliverables are accepted when they satisfy the agreed Acceptance Criteria or when the applicable review period expires without a valid rejection notice.

7.2 Deliverables Register

Deliverable	Description	Due Date	Acceptance Owner
Project Plan	Detailed implementation activities, responsibilities, dependencies, and milestones	Week 1	Customer Project Manager
Requirements Specification	Confirmed business, functional, technical, and security requirements	Week 2	Customer Contract Manager
Configured Platform	Customer-specific workflows, roles, templates, and dashboards	Week 6	Customer Product Owner
Integration Package	Configured interfaces and technical documentation	Week 8	Customer IT Lead
Test Report	Functional, security, and performance test results	Week 9	Customer IT Lead
Training Materials	Administrator and end-user training content	Week 10	Customer Project Manager
Production Environment	Approved live platform environment	Week 12	Customer Executive Sponsor
Monthly Service Report	Performance, incidents, usage, risks, and planned changes	Monthly	Customer Contract Manager

7.3 Acceptance Criteria

A Deliverable is acceptable where it:

- Materially complies with the agreed specification.
- Performs the required functions.
- Does not contain unresolved Critical defects.
- Meets applicable security requirements.
- Includes required supporting documentation.
- Is provided in the agreed format.
- Can be reasonably used for its intended purpose.

7.4 Acceptance Procedure

The Customer has ten business days after delivery to:

- Accept the Deliverable.
- Reject the Deliverable.
- Accept it subject to agreed minor corrections.
- Request clarification.

A rejection must:

- Be submitted in writing.
- Identify the relevant Acceptance Criterion.
- Describe the defect.
- Include supporting evidence.
- State the expected correction.

The Supplier must correct valid defects and resubmit the Deliverable.

The revised Deliverable is subject to a new five-business-day review period.

7.5 Deemed Acceptance

A Deliverable may be deemed accepted when:

- The Customer uses it in production.
- The Customer does not respond within the review period after receiving a formal reminder.
- The Customer confirms that any remaining issues are minor and do not prevent operational use.

Deemed acceptance does not waive latent defects, security vulnerabilities, fraud, or defects that could not reasonably have been identified during the review period.

7.6 Change Request Process

Either party may submit a Change Request.

Each Change Request must include:

- Description of the requested change.
- Business rationale.
- Scope impact.
- Timeline impact.
- Fee impact.
- Security impact.
- Data protection impact.
- Resource requirements.
- Acceptance criteria.
- Dependencies.

The Supplier must not begin chargeable change work without written approval.

7.7 Emergency Changes

The Supplier may implement an emergency change without prior approval where necessary to:

- Resolve a Critical Incident.
- Address a material security vulnerability.
- Prevent data loss.
- Comply with a mandatory legal requirement.

The Supplier must notify the Customer as soon as reasonably practicable and provide a post-change report.

7.8 Change Control Risk

The Supplier may classify work as either included support or chargeable change work. The agreement does not include a detailed classification matrix.

Recommended Control	Add examples of included configuration, minor enhancements, major enhancements, integrations, and new module development.

8. Commercial Terms, Fees, and Invoicing

8.1 Codified Summary

The Customer must pay a one-time implementation fee and an annual subscription fee.

Additional fees may apply for excess usage, approved Change Requests, additional professional services, and services outside the agreed scope.

8.2 Fee Structure

Fee Category	Amount	Billing Basis
Implementation Fee	EUR 95,000	40% on signature, 30% after configuration, 30% on Go-Live
Annual Subscription Fee	EUR 180,000	Payable annually in advance
Additional Professional Services	EUR 1,250 per consultant day	Monthly in arrears
Additional User Package	EUR 12,000 per 50 users	Annual
Additional Document Volume	EUR 0.18 per page	Quarterly in arrears
On-site Support	EUR 1,500 per consultant day plus approved expenses	Monthly in arrears

8.3 Invoicing Requirements

Invoices must include:

- Supplier legal name.

- Customer legal entity.
- Contract reference.
- Purchase order number, where applicable.
- Description of Services.
- Billing period.
- Applicable milestone.
- Fee calculation.
- Taxes.
- Payment details.

The Customer may reject an invoice that does not contain the required information.

8.4 Payment Terms

Valid and undisputed invoices are payable within 30 calendar days of receipt.

The Customer may withhold only the disputed portion of an invoice.

The parties must attempt to resolve invoice disputes within 15 business days.

The Customer must pay any undisputed balance by the original due date.

8.5 Taxes

Fees exclude value-added tax and equivalent transaction taxes.

The Supplier is responsible for:

- Corporate income taxes.
- Employment taxes.
- Taxes imposed on Supplier Personnel.
- Taxes arising from the Supplier's business operations.

The Customer may deduct withholding taxes where legally required and must provide appropriate supporting documentation.

8.6 Fee Adjustments

Subscription fees remain fixed during the Initial Term.

For a renewal term, the Supplier may increase fees by the lower of:

- Three per cent.
- The annual consumer price index increase.
- Another percentage agreed in writing.

The Supplier must provide at least 120 days' notice of any proposed increase.

8.7 Expenses

Travel and accommodation expenses are reimbursable only where:

- The Customer approves them in advance.
- They are reasonable.
- Supporting receipts are provided.

- They comply with the Customer's travel policy.

8.8 Late Payment

The Supplier may charge statutory interest on overdue undisputed amounts.

The Supplier may not suspend the Services unless:

- An undisputed amount remains unpaid for more than 45 days.
- The Supplier provides at least 15 business days' written notice.
- The Customer fails to remedy the non-payment during the notice period.

8.9 Commercial Risk

The excess document-processing charge is calculated per page, but the agreement does not specify how pages are counted for spreadsheets, images, compressed files, or duplicate uploads.

Recommended Control	Define the page-counting methodology and provide a monthly usage dashboard before excess charges accrue.

9. Confidentiality, Data Protection, and Information Security

9.1 Codified Summary

Each party must protect the other party's Confidential Information.

The Supplier acts as a processor of Personal Data where it processes Personal Data on behalf of the Customer.

Customer Data must be hosted within the European Economic Area unless the Customer provides prior written approval.

9.2 Confidential Information

Confidential Information includes:

- Commercial information.
- Technical information.
- Customer Data.
- Pricing.
- Security documentation.
- Business plans.
- Contract terms.
- Product roadmaps.
- Supplier submissions.
- Internal reports.
- Personal Data.
- Information marked or reasonably understood as confidential.

9.3 Confidentiality Obligations

Each receiving party must:

- Use Confidential Information only for the agreement.
- Restrict access to personnel with a need to know.
- Apply appropriate security measures.
- Prevent unauthorised disclosure.
- Notify the disclosing party of unauthorised access.
- Return or securely delete information when required.

Confidentiality obligations do not apply where the information:

- Is lawfully public.
- Was already known without restriction.
- Is independently developed.
- Is lawfully obtained from another source.
- Must be disclosed by law.

9.4 Data Protection Roles

The Customer acts as controller.

The Supplier acts as processor when processing Personal Data through the Services.

The Supplier must process Personal Data only:

- On documented Customer instructions.
- For the purpose of providing the Services.
- For the duration of the agreement.
- In accordance with the Data Processing Terms.

9.5 Data Processing Requirements

The Supplier must:

- Maintain records of processing.
- Ensure personnel confidentiality.
- Implement appropriate technical and organisational measures.
- Assist with data-subject requests.
- Assist with data protection impact assessments.
- Notify the Customer of a Personal Data breach.
- Delete or return Personal Data at the end of the Services.
- Provide compliance information.
- Permit audits subject to reasonable conditions.

9.6 Security Controls

Required controls include:

- Encryption in transit.

- Encryption at rest.
- Multi-factor authentication.
- Role-based access control.
- Secure software-development practices.
- Vulnerability scanning.
- Penetration testing.
- Security logging.
- Malware protection.
- Backup and recovery.
- Incident-response procedures.
- Privileged-access management.
- Personnel security training.

9.7 Security Incident Notification

The Supplier must notify the Customer without undue delay and no later than 24 hours after confirming a material security incident affecting Customer Data.

The initial notification must include available information concerning:

- Nature of the incident.
- Systems affected.
- Data affected.
- Estimated number of records.
- Potential consequences.
- Containment measures.
- Planned remediation.
- Contact person.

The Supplier must provide updates until closure and deliver a written root-cause report.

9.8 Data Retention

Customer Data is retained:

- For the duration of the agreement.
- For up to 30 days after termination to support export and transition.
- For an additional 60 days in encrypted backup systems.

After the retention period, the Supplier must securely delete the data unless retention is legally required.

9.9 Use of Artificial Intelligence

The Supplier may use artificial intelligence models to process Customer documents solely for the purpose of providing the Services.

The Supplier must not:

- Use Customer Data to train publicly available models.
- Use Customer Data to improve services for unrelated customers without consent.

- disclose Customer Data to external model providers without appropriate contractual controls.
- Make Customer Data available through public interfaces.

Generated outputs must be traceable to source documents wherever technically feasible.

9.10 Information Security Risk

The agreement refers to annual penetration testing but does not specify whether the Customer receives the complete report or only a summary.

Recommended Control	Require an executive summary, evidence of remediation, and disclosure of unresolved Critical and High-risk findings.

10. Intellectual Property, Warranties, and Usage Rights

10.1 Codified Summary

The Supplier retains ownership of the Platform, underlying software, methodologies, models, generic templates, and pre-existing intellectual property.

The Customer retains ownership of Customer Data, Customer Materials, and Customer-specific content.

10.2 Supplier Intellectual Property

Supplier intellectual property includes:

- Platform source code.
- Software architecture.
- Generic workflows.
- Algorithms.
- General-purpose templates.
- Libraries.
- Connectors.
- Documentation.
- Technical methods.
- Pre-existing tools.
- Product improvements of general application.

No ownership of Supplier intellectual property transfers to the Customer.

10.3 Customer Intellectual Property

Customer intellectual property includes:

- Customer Data.
- Internal policies.
- Procurement templates.
- Evaluation methodologies supplied by the Customer.
- Contracting standards.
- Supplier information.

- Customer-specific reports.
- Customer branding.

The Supplier receives a limited licence to use Customer intellectual property only to provide the Services.

10.4 Customer-Specific Deliverables

The Customer owns the final Customer-specific reports and structured outputs generated using Customer Data.

The Supplier retains ownership of:

- Generic report structures.
- Reusable code.
- Generic data models.
- Underlying templates.
- Technical components used to generate the Deliverables.

The Customer receives a perpetual right to use accepted Customer-specific Deliverables for its internal business purposes.

10.5 Platform Licence

The Supplier grants the Customer a:

- Non-exclusive.
- Non-transferable.
- Non-sublicensable.
- Time-limited.
- Internal-use licence.

The licence applies only during the contract term and only to authorised entities and users.

10.6 Feedback

The Supplier may use general feedback provided by the Customer to improve the Platform.

The Supplier may not:

- Identify the Customer publicly.
- disclose Customer Confidential Information.
- Reproduce Customer-specific workflows for another customer.
- Use Customer Data when applying feedback.

10.7 Supplier Warranties

The Supplier warrants that:

- It has authority to enter into the agreement.
- The Services will materially conform to the agreed specification.
- Professional Services will be delivered with reasonable skill and care.
- It will not knowingly introduce malicious code.
- It has the rights required to provide the Services.

- It will comply with applicable laws.
- It will maintain required licences and permissions.

10.8 Customer Warranties

The Customer warrants that:

- It has authority to enter into the agreement.
- It has lawful rights to provide Customer Data.
- Its instructions will not knowingly require unlawful processing.
- Authorised Users will comply with the agreement.

10.9 Third-Party Claims

The Supplier must defend the Customer against third-party claims alleging that the authorised use of the Platform infringes intellectual property rights.

The Supplier may:

- Obtain continued usage rights.
- Modify the affected component.
- Replace the affected component.
- Terminate the affected Service and refund prepaid fees where no reasonable alternative exists.

10.10 Intellectual Property Risk

The agreement allocates ownership of Customer-specific outputs but does not clearly address ownership of jointly designed workflows.

Recommended Control	Distinguish between Customer-exclusive configurations, Supplier reusable components, and jointly developed intellectual property.

11. Service Levels, Liability, and Risk Allocation

11.1 Codified Summary

The Supplier must meet defined availability, support-response, incident-resolution, backup, and recovery commitments.

Service credits apply where specified Service Levels are missed.

Service credits are not the Customer's exclusive remedy for persistent or material failure.

11.2 Availability Commitment

The Platform must achieve **99.5% monthly availability**.

Availability excludes:

- Approved planned maintenance.
- Customer systems or network failures.
- Force majeure events.
- Customer misuse.

- Emergency security maintenance.
- Third-party systems outside the Supplier's control, where reasonable continuity measures have been implemented.

11.3 Incident Severity Levels

Severity	Description	Response Target	Restoration Target
Critical	Complete outage, confirmed material breach, or loss of critical functionality	30 minutes	4 hours
High	Major degradation affecting multiple users or essential workflows	1 hour	8 hours
Medium	Limited functionality with available workaround	4 business hours	3 business days
Low	Minor issue with limited operational impact	1 business day	Next planned release

11.4 Service Credits

Where monthly availability falls below the target:

Monthly Availability	Service Credit
99.0%–99.49%	5% of monthly subscription fee
98.0%–98.99%	10% of monthly subscription fee
95.0%–97.99%	20% of monthly subscription fee
Below 95.0%	30% of monthly subscription fee

The total service credit for a month cannot exceed 30% of the applicable monthly subscription fee.

11.5 Persistent Failure

Persistent failure occurs where:

- Availability falls below 98% in two consecutive months.
- A Critical Incident remains unresolved for more than 24 hours.
- Three or more Critical Incidents occur in a rolling three-month period.
- The Supplier repeatedly fails to meet material security obligations.

Persistent failure may constitute a material breach.

11.6 Backup and Recovery

The Supplier must maintain:

- Daily encrypted backups.
- Geographically separate backup storage.
- A recovery point objective of four hours.
- A recovery time objective of eight hours.

- Annual disaster recovery testing.

11.7 Liability Cap

Each party's aggregate liability is capped at the fees paid or payable during the 12 months preceding the event giving rise to the claim.

The liability cap does not apply to:

- Fraud.
- Wilful misconduct.
- Death or personal injury caused by negligence.
- Unauthorised use of the other party's intellectual property.
- Breach of confidentiality.
- Certain data protection liabilities.
- Amounts that cannot legally be limited.

11.8 Excluded Losses

Neither party is liable for:

- Indirect loss.
- Consequential loss.
- Loss of anticipated profit.
- Loss of business opportunity.
- Loss of goodwill.

However, the following are treated as direct losses where reasonably incurred:

- Data-restoration costs.
- Incident investigation costs.
- Regulatory response costs.
- Replacement-service costs.
- Customer notification costs.
- Reasonable transition costs arising from Supplier breach.

11.9 Insurance

The Supplier must maintain:

- Professional indemnity insurance.
- Cyber liability insurance.
- Public liability insurance.
- Employer's liability insurance.

Evidence of insurance must be provided on request.

11.10 Force Majeure

A party is not liable for delay caused by an event outside its reasonable control, provided that it:

- Notifies the other party.

- Uses reasonable mitigation measures.
- Continues unaffected obligations.
- Activates continuity arrangements.
- Provides regular status updates.

Payment obligations for Services already provided are not suspended by force majeure.

11.11 Liability Risk

The general liability cap may be insufficient for a serious security incident involving large volumes of sensitive procurement or employee data.

Recommended Control	Introduce a higher separate liability cap for confidentiality, cybersecurity, and data protection breaches.

12. Termination, Exit Assistance, and Dispute Resolution

12.1 Codified Summary

Either party may terminate the agreement for material breach, insolvency, prolonged force majeure, or other specified events.

The Customer may terminate for convenience after the Initial Term by providing 90 days' written notice.

The Supplier must provide reasonable exit and transition assistance.

12.2 Termination for Cause

A party may terminate where the other party:

- Commits a material breach that is not remedied within 30 days.
- Commits a breach that cannot be remedied.
- Becomes insolvent.
- Ceases business operations.
- Repeatedly breaches material obligations.
- Engages in fraud or serious misconduct.
- Causes a material regulatory or security risk.

For an urgent security or legal breach, a shorter remediation period may apply.

12.3 Termination for Convenience

The Customer may terminate after the Initial Term with 90 days' written notice.

The Customer must pay:

- Fees due up to the termination date.
- Approved non-cancellable third-party costs.
- Approved transition fees.
- Any outstanding undisputed invoices.

The Customer is not required to pay subscription fees for periods after the termination date.

12.4 Suspension

The Supplier may suspend affected Services where:

- Continued operation creates an immediate security risk.
- The Customer uses the Services unlawfully.
- An undisputed invoice remains unpaid after the applicable notice period.
- Suspension is required by law.

Suspension must be proportionate and limited to the affected Service or user wherever possible.

12.5 Exit Assistance

The Supplier must provide:

- Export of Customer Data.
- Export of Customer-specific reports.
- Current configuration documentation.
- User and permission lists.
- Open-incident information.
- Integration documentation.
- Data-retention confirmation.
- Knowledge-transfer sessions.
- Reasonable cooperation with a replacement supplier.

Data must be exported in commonly used formats, including CSV, XLSX, JSON, PDF, or DOCX, depending on the relevant data type.

12.6 Exit Period

The standard exit period is 60 days following termination.

The Customer may request an extension of up to 90 additional days.

Exit assistance is charged at the agreed professional-service rates unless termination results from an uncured Supplier material breach.

12.7 Data Deletion

Following completion of the exit period, the Supplier must:

- Delete active Customer Data.
- Revoke user access.
- Disable integrations.
- Remove Customer credentials.
- Provide written deletion confirmation.
- Delete backup copies in accordance with the backup-retention cycle.

12.8 Continuing Provisions

The following obligations survive termination:

- Confidentiality.

- Data protection.
- Intellectual property.
- Payment obligations.
- Liability.
- Audit rights relating to the contract period.
- Dispute resolution.
- Data deletion.
- Exit obligations.

12.9 Dispute Escalation

Disputes follow this sequence:

1. Operational representatives attempt resolution.
2. Contract managers meet within five business days.
3. Executive sponsors meet within ten business days.
4. The parties attempt mediation.
5. Unresolved disputes proceed to confidential arbitration.

The parties must continue performing undisputed obligations during the dispute.

12.10 Arbitration

Arbitration is conducted:

- By a single arbitrator.
- In English.
- In the fictional city of Bellmont.
- Under the fictional Norland Commercial Arbitration Rules.
- On a confidential basis.

Either party may seek urgent injunctive relief from a competent court to protect Confidential Information, Personal Data, or intellectual property.

12.11 Exit Risk

Exit support is available, but the agreement does not define the maximum volume of data, number of knowledge-transfer sessions, or required response times during transition.

Recommended Control	Add a detailed Exit Services Plan with fixed Deliverables, owners, formats, deadlines, and pricing.

Consolidated Obligations Register

ID	Responsible Party	Obligation	Due Date / Frequency	Criticality
OBL-001	Supplier	Deliver Project Plan	Week 1	High

ID	Responsible Party	Obligation	Due Date / Frequency	Criticality
OBL-002	Customer	Confirm requirements	Week 2	High
OBL-003	Supplier	Complete platform configuration	Week 6	Critical
OBL-004	Customer	Complete user acceptance testing	Week 11	Critical
OBL-005	Supplier	Achieve production Go-Live	Week 12	Critical
OBL-006	Supplier	Maintain 99.5% monthly availability	Monthly	Critical
OBL-007	Supplier	Provide service report	Monthly	Medium
OBL-008	Supplier	Conduct disaster recovery test	Annually	High
OBL-009	Supplier	Notify material security incidents	Within 24 hours of confirmation	Critical
OBL-010	Customer	Pay valid invoices	Within 30 calendar days	High
OBL-011	Supplier	Notify proposed renewal fees	120 days before renewal	Medium
OBL-012	Customer	Provide non-renewal notice	90 days before term expiry	High
OBL-013	Supplier	Maintain approved insurance	Throughout the Term	High
OBL-014	Customer	Deactivate unauthorised users	Promptly	High
OBL-015	Supplier	Export Customer Data following termination	During the Exit Period	Critical

Deliverables Register

Deliverable	Format	Owner	Acceptance Method	Status
Project Plan	XLSX / PDF	Supplier	Written approval	Not Started
Requirements Specification	DOCX / PDF	Supplier	Written approval	Not Started
Configured Platform	Hosted Environment	Supplier	User acceptance testing	Not Started
Integration Documentation	DOCX / PDF	Supplier	Technical review	Not Started
Test Report	PDF	Supplier	Customer IT approval	Not Started

Deliverable	Format	Owner	Acceptance Method	Status
Training Materials	PPTX / PDF	Supplier	Training completion	Not Started
Monthly Service Report	PDF / XLSX	Supplier	Operational review	Recurring
Data Export Package	CSV / XLSX / JSON	Supplier	File validation	On Termination
Deletion Certificate	PDF	Supplier	Written confirmation	On Termination

Key Dates and Deadlines

Event	Date or Timing	Action Required
Effective Date	15 March 2026	Agreement becomes effective
Project Kick-off	Within 5 Business Days	Appoint project team
Requirements Approval	End of Week 2	Customer approval
Configuration Completion	End of Week 6	Supplier delivery
User Acceptance Testing	Weeks 9–11	Customer testing
Production Go-Live	End of Week 12	Final approval
Monthly Service Report	Fifth Business Day of each month	Supplier submission
Renewal Notification	120 days before term expiry	Supplier notice
Non-Renewal Deadline	90 days before term expiry	Either party notice
Initial Term Expiry	14 March 2028	Renewal or termination decision

Key Commercial Commitments

Commercial Item	Contract Position
Implementation Fee	EUR 95,000
Annual Subscription Fee	EUR 180,000
Subscription Billing	Annual, in advance
Payment Period	30 calendar days
Included Users	150
Included Administrators	20
Included Document Volume	50,000 pages per year
Professional Services Rate	EUR 1,250 per consultant day

Commercial Item	Contract Position
Maximum Annual Fee Increase	Lower of 3% or applicable consumer price index
Service Credit Cap	30% of monthly subscription fee
General Liability Cap	100% of preceding 12 months' fees

Contract Risk Summary

Risk ID	Risk Description	Severity	Recommended Action
RSK-001	Financial approval authority for operational instructions is unclear	High	Establish approval thresholds
RSK-002	Scope distinction between configuration and development is subjective	High	Add scope classification matrix
RSK-003	Deemed acceptance may apply after a short review period	Medium	Introduce reminder and cure period
RSK-004	Customer dependencies are not consolidated	Medium	Create dependency register
RSK-005	Excess document-volume calculation is unclear	Medium	Define page-counting rules
RSK-006	Penetration-testing reporting requirements are limited	High	Require findings summary and remediation evidence
RSK-007	Jointly developed intellectual property is not clearly allocated	High	Add joint-development provisions
RSK-008	Cybersecurity liability cap may be insufficient	Critical	Introduce enhanced security liability cap
RSK-009	Exit-assistance scope is not quantified	High	Agree detailed Exit Services Plan
RSK-010	Subjective terms are used without measurable thresholds	Medium	Add definitions and objective criteria

Final Codification Summary

The agreement establishes a managed enterprise technology relationship under which the Supplier will implement and operate a procurement intelligence platform for the Customer.

The contractual structure is generally comprehensive and addresses implementation, platform operation, professional services, data processing, security, service levels, commercial terms, intellectual property, liability, and termination.

The most significant contractual dependencies concern:

- Timely Customer approvals.
- Accurate and lawful Customer Data.
- Clear classification of additional work.
- Compliance with security and data protection requirements.
- Achievement of implementation and availability targets.
- Effective exit planning.

The principal areas requiring further clarification are:

1. Financial authority for operational instructions.
2. Boundaries between included support and chargeable development.
3. Treatment of jointly developed workflows.
4. Measurement of document-processing volumes.
5. Enhanced liability for data protection and cybersecurity events.
6. Quantification of exit and transition support.

Subject to resolution of these matters, the agreement provides a workable framework for the implementation and ongoing operation of the Services.