DATA PROTECTION AGREEMENT
(Data Protection Agreement)

Section 1

Clause 1 – Purpose

This Data Protection Agreement sets out the conditions under which the Processor undertakes to process, on behalf of the Controller, the personal data necessary for the operation of the Tevasoft modules, including EVA Controls, Multi VAT, Smart Extract and Connect:

- the capture, analysis and verification of expense receipts;
- the performance of automated compliance, fraud detection or expense policy controls;
- data extraction using OCR or a large language model where necessary;
- the identification and structuring of VAT information, including where multiple VAT rates apply;
- the search, extraction, consultation and export of data and supporting documents;
- the transformation, mapping and transmission of data between systems;
- the validation of company identifiers such as SIREN, SIRET, VAT numbers or any other applicable identifier;
- the generation of reports, alerts, export files or integration flows;
- the processing of any other field necessary for the operation of the modules subscribed to by the Client.

Clause 2 - Invariability of the Clauses

The Parties undertake not to amend the Clauses, except by adding information to the Annexes or updating the information contained therein.

The Parties are not, however, prevented from including the standard contractual clauses set out herein in a broader agreement, or from adding other clauses or additional safeguards, provided that these do not directly or indirectly contradict the Clauses or prejudice the fundamental rights and freedoms of data subjects.

Clause 3 – Interpretation

Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively appear in these Clauses, they shall be interpreted in accordance with the relevant Regulation.

These Clauses shall be read and interpreted in the light of the provisions of Regulations (EU) 2016/679 and 2018/1725 respectively.

These Clauses shall not be interpreted in a manner that conflicts with the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, or in a manner that prejudices the fundamental rights and freedoms of data subjects.

Clause 4 – Hierarchy

In the event of any inconsistency between these Clauses and the provisions of related agreements between the Parties existing at the time these Clauses are signed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Term

This Agreement shall enter into force on the date of signature and shall remain valid throughout the contractual term for the provision of the Tevasoft modules subscribed to by the Client, plus the period required to fulfil the data deletion or return obligations set out in Clause 16.

Section 2 – Obligations of the Parties

Clause 6 – Description of Processing

Details of the processing operations, and in particular the categories of personal data and the purposes for which personal data is processed on behalf of the Controller, are set out in Annex 1.

Clause 7 – Obligations of the Processor

- Process personal data only on documented instructions from the Controller;
- Ensure data confidentiality and train authorized personnel;
- Implement the appropriate technical and organizational measures detailed in Annex 2;
- Assist the Controller in meeting its obligations regarding data subject rights (Articles 12 to 22 GDPR) and data protection impact assessments (Article 35 GDPR);
- Notify the Controller of any personal data breach within 24 hours of discovery, in accordance with Clause 8;
- Maintain a record of categories of processing activities (Article 30(2) GDPR);
- Allow for and contribute to audits, including inspections, conducted by the Controller or an auditor appointed by it (Clause 12);
- Inform the Controller of any intended changes concerning the addition or replacement of Sub-processors (Clause 10).

Clause 8 – Obligations of the Controller

- Ensure that there is a lawful basis for the processing and provide appropriate information to data subjects;
- Provide the Processor with lawful and documented instructions;
- Cooperate with the Processor in carrying out impact assessments or responding to supervisory authorities;
- Supervise the activities of the Processor and Sub-processors.

Clause 9 – Technical and Organizational Security Measures

The Processor undertakes to implement, at a minimum, the measures described in Annex 2.

Clause 10 – Personal Data Breach Notification

In the event of a personal data breach, the Processor shall:

- Inform the Controller without undue delay and, in any event, within 24 hours of discovery;
- Provide all useful information enabling the Controller to assess the scope, impact and necessary remedial actions;
- Cooperate with the Controller regarding any notification to supervisory authorities and data subjects.

Clause 11 – Sub-processing

The Processor may engage a Sub-processor only with the Controller's written authorization. The currently authorized Sub-processors are listed in Annex 3. The Processor shall impose obligations on each Sub-processor that are at least equivalent to its own obligations.

Clause 12 – Data Transfers Outside the EU/EEA

Any transfer to a third country shall be subject to:

- an adequacy decision of the European Commission;
- or approved Standard Contractual Clauses;
- or another mechanism compliant with Articles 46 to 49 of the GDPR.

The Processor undertakes to provide supporting documentation upon request.

Clause 13 – Audit Rights

The Controller may, once (1) per year and subject to reasonable prior notice of thirty (30) days, conduct or have conducted an audit of the processing activities covered by this Agreement. Audit costs shall be borne by the Controller, except in the event of a proven material breach by the Processor.

Clause 14 – Confidentiality

The Parties acknowledge that personal data and information relating to security measures constitute confidential information.

Clause 15 – Assistance and Cooperation

In the event of a personal data breach concerning data processed by the Processor, the Processor shall inform the Controller without undue delay after becoming aware of it. Such notification shall include at least:

- a description of the nature of the breach identified (including, where possible, the categories and approximate number of data subjects and personal data records affected);
- the contact details of a contact point from whom further information concerning the breach may be obtained;
- its likely consequences and the measures taken or proposed to address the breach, including measures intended to mitigate any possible adverse effects.

Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available, and further information shall be provided subsequently as soon as it becomes available.

Clause 16 – Term and Disposal of Data

Upon expiry or termination of the service agreement, the Processor shall, at the Controller's choice:

1. Delete or return all personal data processed on behalf of the Controller.
2. Return all personal data and destroy all existing copies, unless Union or national law requires storage of the personal data for a longer period.

The Processor shall continue to ensure compliance with these Clauses until the data has been fully deleted or returned.

Written confirmation of deletion shall be provided to the Controller.

Clause 17 – Governing Law and Jurisdiction

This Agreement shall be governed by French law. Any dispute shall be subject to the exclusive jurisdiction of the courts having jurisdiction over the Controller's registered office, unless mandatory law provides otherwise.

Section 3 – Final Provisions

Clause 18 – Non-compliance with the Clauses and Termination

Without prejudice to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the Processor fails to comply with its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the Processor complies with these Clauses or the agreement is terminated. The Processor shall promptly inform the Controller if it is unable to comply with these Clauses, for any reason.

The Controller shall be entitled to terminate the agreement, insofar as it concerns the processing of personal data under these Clauses, where:

1. the processing of personal data by the Processor has been suspended by the Controller and compliance with these Clauses is not restored within a reasonable time and, in any event, within one month of suspension;
2. the Processor is in substantial or persistent breach of these Clauses or of its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
3. the Processor fails to comply with a binding decision of a competent court or one or more competent supervisory authorities regarding its obligations under these Clauses or Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

The Processor shall be entitled to terminate the agreement, insofar as it concerns the processing of personal data under these Clauses, where, after informing the Controller that its instructions infringe applicable legal requirements, the Controller insists that the instructions be followed.

Following termination of the agreement, the return or deletion provisions set out in Clause 16 shall apply.

Signature :

Client Name	
Signatory Name	
Position	
Date	
Signature	

Annex 1 - Detailed Description of Processing

Module	Main Purpose	Processing Operations
EVA Controls	Control, validation and compliance of business expenses	Collection of supporting documents, OCR/LLM extraction, compliance checks, fraud detection, SIREN/SIRET verification, address checks, amount checks, keyword detection, supporting-document format checks, application of the expense policy, generation of alerts and reports
Multi TVA	Identification and structuring of VAT information relating to business expenses	Analysis of supporting documents, identification of VAT rates, extraction of net/gross/VAT amounts, structuring of tax data, updating or transmission of VAT fields to the source system
Smart Extract	Search, extraction and export of data and supporting documents	Data search, extraction of supporting documents, generation of PDF/Excel/CSV/JSON/XML exports, scheduling of exports, secure availability of files
Connect	Integration, transformation and transmission of data between systems	Receipt of data, mapping, transformation, consistency checks, transmission to SAP Concur, client systems or external platforms, status monitoring, and management of integration errors

Categories of Personal Data Processed:

Data Category	Processed under the Agreement?	Details
Civil status, identity and identification data	Yes	Last name, first name, identifier, email address, country of residence, user identifier in the source system, employee identifier, supplier or third-party identifier where applicable.
Identification of a personal or company vehicle	Yes	Vehicle registration number and fiscal horsepower
Personal life (lifestyle, family situation, excluding sensitive data)	No	

Professional life (CV, training, qualifications, distinctions, etc.)	Yes	Assignment within the company (employment, affiliation to a company, department, cost center or any other organizational level) Last name, first name, position and company of external guests invited in a professional context (business meals, events, gifts)
Economic and financial information (income, tax situation, etc.)	No	
Connection data (IP addresses, event logs, etc.)	Yes	Connection logs
Location data (travel, GPS, GSM data, etc.)	No	
Bank details	No	No, unless a specific Connect flow containing such information is activated, in which case the processing will be documented contractually.
Other types of data	Yes	Business expense receipts, supporting documents, billing data, VAT data, invoice numbers, tax or commercial identifiers, data from exports or integration flows.

Sensitive Data (Special Categories)

Data Category	Processed under the Agreement?	Details
Biometric data	No	
Philosophical beliefs	No	
Political opinions	No	
Religious beliefs	No	
Trade union membership	No	
Sex life or sexual orientation	No	

Health data	No	
Genetic data	No	
Social security number	No	
Data relating to criminal convictions or offences	No	

Retention period: 10 years from the end of the relevant fiscal year for data having accounting or tax value, unless otherwise required by law or instructed by the Client in documented form. Technical logs and event logs are retained for the period specified in Annex 2.

Annex 2 - Technical and Organizational Measures

Encryption	● Data at rest: AES-256. ● Data in transit: TLS 1.3.
Access Control	● SSO login ● Role-based access control (RBAC) applying the principle of least privilege.
Logging and Monitoring	● Timestamped, immutable logs retained for 1 month.
Security Testing	● Annual vulnerability scan. ● Annual penetration test by a qualified third party.
Business Continuity	● Daily backups, 30-day retention, off-site storage.
Artificial Intelligence Governance	● Where Tevasoft modules use OCR, LLM or automated analysis processing, such processing is reviewed regularly, including assessment of performance, error risks, potential bias and associated control measures.

Annex 3 – Authorized Sub-processors

Company	Services Provided	Data Location	Transfer Mechanism	Notes
CleverCloud	Application hosting, database, cloud infrastructure and backups for Tevasoft modules	France, Paris	None (EU)	ISO 9001 ISO 27001 : 2022 SecNumCloud
Mistral AI	Large language model service used for certain document analysis or extraction processes, depending on the modules activated.	EU	None (EU)	ISO 27001:2022 ISO 27701 SOC 2
Sightengine	Service for detecting receipts or supporting documents potentially generated by artificial intelligence, primarily as part of automated controls.	Data not stored	Standard Contractual Clauses	ISO 27001:2022 SOC 2 PCI DSS