Appendix- Common provisions for the processing of Personal Data

1. Definitions

For the purposes of this appendix, all the definitions set out in (EU) Regulation 2016/679 (DPR) shall apply.

"**Data Protection Laws**" refers to any law or regulation relating to data protection and cyber security that governs the processing of Personal Data under the Contract, including (EU) Regulation 2016/679 (GDPR) and specific national data protection legislation applying to the Customer and Expensya.

2. Purpose

This document forms part of the appendices to the Terms and Conditions and constitutes the “Common provisions for the processing of Personal Data” between the Service Provider and the Customer.

3. Interpretation

A reference to a statute or legal provision includes a reference to any subordinate legislation and also constitutes a reference to that statute, legal provision or subordinate legislation in connection with any amendment, unification, re-enactment, re-numbering or replacement (with or without amendment) of the latter after the date of the appendix and any statute, legal provision or subordinate legislation that it purports to unify, re-enact or replace (with or without amendment).

References in the singular include the plural and vice versa.

The terms following the terms/expressions "includes", "include", "including", "notably", "in particular" or similar terms and expressions shall be interpreted without restriction and therefore shall not limit the meaning of the preceding terms.

4. Commitment of the Service Provider in its capacity as Data processor

Unless otherwise agreed between the Parties in writing, the Service Provider shall process the Personal Data for the sole purpose of performing its obligations under these Terms and Conditions or for any other purpose expressly authorized in the Contract in accordance with applicable Data Protection Laws, under the supervision of the Customer in its capacity as Data Controller.

The Service Provider shall not process Personal Data in a manner which is incompatible with the Data Protection Laws applying to the Service Provider and/or the Customer.

In particular, the Service Provider undertakes to:

- Process Personal Data solely for the purpose(s) set forth in the Contract;
- Process Personal Data in accordance with the Customer's documented instructions;
- Guarantee the confidentiality of the Personal Data processed under the Contract;

- Ensure that the persons authorized to process Personal Data under the Contract:
    - Undertake to respect confidentiality or are subject to an appropriate legal confidentiality obligation,
    - Receive the necessary training in relation to the protection of Personal Data.
- With respect to the design of its tools, products, applications or services, take into account data protection principles from the outset as well as default data protection principles;
- Inform the Customer prior to any processing if the Service Provider is required by law to process Personal Data other than in accordance with the Customer's instructions, unless the relevant law prohibits such processing for reasons of public interest, in which case the Service Provider shall inform the Customer as soon as the law permits;
- Assist the Customer in fulfilling its obligations under Data Protection Laws, including its obligation to comply with requests to exercise the rights of Data Subjects. This assistance shall be provided in such a way as to enable the Customer to meet its obligations fully in a timely manner;
- Cooperate with the Customer in the establishment and updating of the Customer's processing activity log, but only for the processing activities performed by the Service Provider on behalf of the Customer under these Terms and Conditions.

In accordance with the commitments set out above, if the Service Provider considers that an instruction from the Customer constitutes a breach of the applicable Data Protection Laws, it shall immediately inform the Customer thereof.

In addition, if the Service Provider is required to transfer Data to a third country or to an international organization under Data Protection Laws, it must inform the Customer of this legal obligation prior to processing, unless the relevant law prohibits such information for important reasons of public interest.

The Service Provider further warrants that it has no reason to believe that legislation concerning it or its activities prevents it from complying with the instructions given by the Customer or from fulfilling its obligations hereunder. If a change in legislation is likely to have a significant negative impact on the guarantees and obligations set out in this appendix or if the Service Provider considers that the Customer's instructions constitute a breach of Data Protection Laws or decisions by a supervisory authority, the Service Provider shall inform the Customer as soon as it becomes aware of such a change.

The Service Provider shall keep a record of the personnel and service providers authorized to process Personal Data and shall ensure that such personnel and their subcontractors:

- Are bound by confidentiality obligations identical to those between the Customer and the Service Provider and set out in these Terms and Conditions;
- Have received appropriate training and are subject to appropriate supervision with regard to the processing of Personal Data;
- Have access to Personal Data which is strictly limited to the necessary requirements for the performance of the Services and/or Expensya's obligations under these Terms and Conditions.

5. Security measures

The Service Provider has implemented and shall maintain appropriate technical, physical and organizational measures (including by imposing a confidentiality clause on its employees, agents and subcontractors) to protect Personal Data from accidental or unlawful destruction, accidental loss, alteration or unauthorized disclosure or access.

The Service Provider shall promptly inform the Customer if it becomes aware of any security incident, unauthorized access, misappropriation, loss, damage or other actual or alleged compromise relating to the security, confidentiality or integrity of the Personal Data processed by its employees, in its capacity as Data Processor.

If a security breach is detected, the Service Provider shall take all necessary measures to prevent another potential breach and shall promptly provide the Customer with all the assistance required to fulfil its information obligations as Data Controller.

In addition, the Service Provider has appointed a Data Protection Officer (DPO) and shall ensure that this DPO is able to carry out his or her duties in compliance with Data Protection Laws.

Contact details of the Service Provider's DPO:
Virtual DPO SAS
42 rue Manin 75019 Paris
RCS 830 490 603 Paris
Email: contact@virtual-dpo.fr

6. Cooperation

6.1. General provisions

At the Customer's written request, the Service Provider shall provide the latter without delay with any useful information in its possession to enable it to meet the requirements of the Data Protection Laws.

The Service Provider's compliance audit conducted by its DPO provides a description of the technical, physical and organizational measures implemented by the Service Provider to protect the Personal Data from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and includes the Service Provider's Data processing activity log for the Customer.

The Service Provider shall provide an electronic copy of the compliance audit within ten (10) working days at the latest at the written request of the Customer.

The Service Provider has chosen not to carry out a Privacy Impact Assessment (PIA) with respect to the characteristics and specific features of its Solution. The Service Provider shall nevertheless provide the appropriate equipment and technical support if the Customer requires an impact analysis to be carried out on the processing operations carried out by the Service Provider in its capacity as Data processor. The Parties agree that the cost of the impact assessment shall be borne exclusively by the Customer, in its capacity as Data Controller. If necessary, the Service Provider may charge the Customer for the time spent and the personnel and equipment used to carry out this analysis, which the Customer understands and accepts.

6.2. Requests from data subjects

The Service Provider shall respond to requests from Data Subjects relating to their Personal Data in accordance with the Customer's instructions:

If the Customer has requested that all requests be transferred to its own services, the Service Provider shall refrain from responding directly to the Data Subjects and shall redirect these requests to the dedicated contact person at the address indicated by the Customer in the Contract;

If the Customer has requested that the Service Provider respond to all requests on its behalf, the Service Provider shall endeavor to provide accurate responses to the best of its knowledge and ability. If it is impossible to answer the questions due to a lack of information, the Service Provider shall transfer the requests to the dedicated contact person at the address indicated by the Customer in the Contract.

The Service Provider shall inform the Customer without delay of requests from Data Subjects to exercise their rights under the Data Protection Laws.

6.3. Data Breach

In the event of a breach of Personal Data, the Service Provider shall inform the Customer as soon as possible and no later than thirty-six (36) hours after becoming aware of such breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise processed.

As soon as possible after the notification of the violation of the Personal Data and as far as possible, the Service Provider shall provide the Customer with the following information:

The categories and approximate number of Persons affected by the violation;

The categories and approximate number of Personal Data records concerned;

A description of the likely consequences of the breach of Personal Data;

A description of the steps taken or proposed by the Service Provider to remedy the breach of the Personal Data including, where appropriate, measures to mitigate any adverse consequences.

If the Service Provider does not have all the information provided for in the preceding paragraph at the time of the initial notification, it shall include in the initial notification the information in its possession at the time of the communication and shall then transmit the missing information as soon as possible.

7. Third party access to Data - subsequent processors

The Service Provider shall ensure that its employees, representatives and subcontractors respect and preserve the integrity, confidentiality and security of the Personal Data.

In the event of subcontracting, the Service Provider undertakes to impose a contractual level of obligation on its subcontractors which is at least equivalent in terms of Data protection to that provided for in this appendix and in the Data Protection Laws. The Service Provider shall remain solely liable towards the Customer for the performance by its subcontractors of their obligations.

The Service Provider shall provide the Customer in the **Data Processing Log** appendix with a list of its current subcontractors who may carry out data processing activities directly or indirectly on all or part of the Customer's Data and the latter has authorized the Service Provider to use the services of these subcontractors.

The Service Provider undertakes only to use the subcontractors' services if they are absolutely necessary for the performance of the Contract.

The Service Provider undertakes only to use subcontractors who:

- Are based in a member country of the European Union or the European Economic Area; or,

- Are based in a country which is considered by the European Commission to offer an adequate level of protection under Data Protection Laws; or,
- Certified under a similar mechanism which is recognized by the European Commission as providing an adequate level of security; or,
- Offer the appropriate guarantees under Article 46 of the GDPR.

8. International Transfers of Personal Data

If the Service Provider transfers Personal Data directly or indirectly outside the European Union or if a subcontractor to be appointed by the Service Provider is likely to transfer Personal Data outside the European Union or in a country that does not guarantee an adequate level of protection within the meaning of the Data Protection Laws, access to such data will only be possible after obtaining the Customer's consent and implementing the appropriate guarantees provided for in Article 46 of the GDPR.

The Service Provider's subsidiary, SARL Expensya Tunisie ((Pepinotech Tunisia), which is 99.92% owned by SA Expensya, is located in Tunisia. The subsidiary, which is in charge of IT development and support, may access Personal Data in the context of the specific services it provides in connection with the Solution. Expensya SA and Expensya Tunisia have signed standard contractual clauses which guarantee that Personal Data can be transferred in accordance with Data Protection Laws.

The Customer acknowledges that he/she has been informed of the latter and accepts that Expensya's subsidiary is located in Tunisia and may have access to Personal Data.

The Service Provider shall provide an electronic copy of the contractual clauses signed with the subcontractor SARL Expensya Tunisie (Pepinotech Tunisia) within ten (10) working days at the latest at the written request of the Customer.

9. Audit

The Service Provider shall provide the Customer upon request with any documents required to demonstrate compliance with its obligations as a subcontractor under these Terms and Conditions. The cost of transmitting these documents by any other means shall be borne by the Customer.

The Customer may request additional explanations from the Service Provider if the documents provided do not enable the Service Provider to verify compliance with the obligations of a subcontractor under these Terms and Conditions or this appendix.

The Customer shall then send a request to the Service Provider, by registered mail with acknowledgment of receipt, in which it justifies and documents its request for additional explanations. The Service Provider undertakes to respond to the Customer as soon as possible.

If, despite the Service Provider's response, the Customer disputes the completeness of the information provided or if the security of the Personal Data is at imminent risk, the Customer may carry out an on-site audit under its own responsibility whose terms are to be agreed upon between the Service Provider and the Customer.

Appendix - Data Processing Activity Log

1. Purpose

This document forms part of the appendices to the Terms and Conditions and constitutes the "Register of Data Processing Activities".

2. Data Processing description

Purpose of processing

☒ The purpose of Data processing by the Subcontractor is defined in particular in the **Service Book** Appendix

☐ Other: ………

Qualification of the risk presented by Processing

Risks	Impacts on individuals	Main sources of risk	Main threats	Existing or planned measures	Seriousness	Likelihood
Unlawful access to data	Visibility in expense reports	Access / password theft	User / password disclosure	SSO	Moderate	Low
Unwanted data amendment	Expense report fraud	Access / password theft	User / password disclosure	SSO / Change Audit	Moderate	Low
Disappearance of data	Loss of data from expense reports, accounting impact	Destruction of Expensya data	Threats external to the supplier	Redundancy, evidence-based archiving	High	Very Low

Duration of processing:

☒ The duration of processing corresponds to the duration of the Contract,

☐ Other: ………

Nature of the processing carried out by the Subcontractor under the Contract includes:

☒ Data collection or recording

☒ Data organization or structuring

☒ Data hosting or storage

☒ Data adaptation or amendment

☒ Data extraction or consultation

☐ Data use

☒ Data communication by transmission, dissemination or any other means of circulation

☐ Data reconciliation or interconnection

☒ Data limitation (blocking)

☒ Data deletion or destruction

☐ Other form of processing:………………..…………………………………………………………………………

Purpose of processing

☒ The purpose of Data processing is defined in the Contract, in particular in the Service Book Appendix.

☐ Other: ………

Data Categories

☒ Name, title, functions

☐ Pictures or recordings such as video or telephone recording

☐ Personal contact data (e.g. telephone, email)

☒ Professional contact data (e.g. company, address, telephone, email)

☐ Personal data (lifestyle, family situation, etc.)

☒ Data relating to working life (CV, vocational training, awards, etc.)

☒ Identification number(s)

☐Contract-related information (contractual relationships, interests in products, services or contracts)

☐ Beneficiary history

☐ Bank details (RIB, IBAN, credit card number, transactions)

☒ Billing or payment data

☐ Evaluation or rating data

☐ Economic and financial information (income, financial situation, tax situation, etc.)

☐ Others: ……………………………………………………………………………

☐ Connection data (IP address, logs, etc.)

☒ Location data (movements, GPS, GSM data, etc.)

Special Data Categories

☐ Data indicating racial or ethnic origin

☐ Data indicating political opinions

☐ Data indicating religious or philosophical convictions

☐ Data indicating union membership

☐ Genetic data

☐ Biometric data for the purpose of uniquely identifying a natural person

☐ Health-related data

☐ Data concerning sexual life or sexual orientation

☐ Data indicating criminal convictions or offenses

☐ Unique National Identification Number (NIR for France)

Categories of persons concerned:

☒ Employees and former employees (salaried workers, trainees)

☐ Visitors

☐ Prospects

☐ Beneficiaries

☐ Others: …………………..

☐ Subscribers

☒ Suppliers, consultants

☐ Sales representatives

☐ Contacts

3. List of authorized subcontractors

#	Name	Address	Country	Processing carried out
1.	Microsoft Azure	Amsterdam	The Netherlands	Storage and hosting of the Expensya solution
2.	Expensya Tunisia	Les Berges du Lac 2, Tunis	Tunisia	Customer Support
3.	CDC Arkhineo	122-120 Rue Réaumur - 75002 PARIS	France	Evidence-based archiving

4. Mapping of data flows outside the European Economic Area or to the United Kingdom

Data flows are only initiated outside the European Economic Area when the Customer issues a request to the Service Provider's support service located in Tunisia. The member of the Service Provider's support team who handled the request then accesses the data specifically mentioned on the Microsoft Azure servers hosted in Amsterdam. No actual data transfer or backup takes place during this procedure.

5. Measures aiming to ensure Data Processing is in compliance with the data protection regulations

5.1. Security

Sub-contractor information systems security policy: available on demand

Encryption:

☒ Key and certificate management procedure

☒ Data encryption

☒ Encryption of data transmissions

☒ Hash function: SHA-256, SHA-512 or SHA-3

☒ Password storage: HMAC utilization of SHA-256, bcrypt, scrypt or PBKDF2

☐ Others: ……………………………………………………… ………………………………

☐ Symmetrical encryption: AES or AES-CBC with 128 bit keys

☐ Signatures: RSA-SSA-PSS as specified in PKCS#1 v2.1
with secret exponents and modules of at least 2048 bits or
3072 bits with public exponents, for encryption,

greater than 65536

Protection of sub-contractor’s computer network:

☐ Limitation of Internet access

☒ Management of Wi-Fi networks

☐ VPN is mandatory for remote access

☒ Administration interfaces are not directly accessible from Internet.

☒ Limitation of network flows

☐ Others: ………………………………………………………………………..

☒ Application of ANSSI recommendations regarding protection of websites, TLS and Wi-Fi

☐ Automatic hardware identification

☒ Set-up of intrusion detection systems

☒ Network partitioning

Traceability:

☒ Set-up of a journaling system

☒ Set-up of specific protection for journaling equipment and journalized information

☒ Set-up of a procedure to monitor use of the Data Processing

☒ Periodic review of event journals

☒ Set-up of a procedure for reporting anomalies or any security incident

☐ Others: ……………………………………….

Management of Authorizations:

☒ Definition of authorization profiles

☒ Deletion of access permits for users as soon as they are no longer authorized to access an IT area or resource, and at the end of their contract

☐ Others: ………………………………………………………….

☒ Performance of an annual authorization review

☒ Set-up of an access control policy

Management of Authentications:

☒ Set-up of a single ID for each user

☒ Prohibition of shared accounts

☒ Compliance with the CNIL recommendation of September 4, 2017 “Authentication by password: elementary security measures

☒ Strong authentication

☒ Limitation on number of access attempts

☒ Password renewal is mandatory

☒ Account blocked if the password is not renewed

☐ Others: ……………………………………………………………………………

☐ Use of password managers to have
different passwords for each department

☒ Secure password storage

☒ Refer to rules and recommendations published by ANSSI concerning authentication mechanisms, whenever strong authentication mechanisms are implemented, particularly annexes B36 and B17 relating
respectively to authentication mechanisms and cryptographic mechanisms

Security Measures:

☒ Use of a regularly updated anti-virus program

☒ Automatic security updating

☒ Search for source and traces of intrusion in the event a station is compromised

☒ Security watch

☒ Encryption of mobile stations and mobile storage media

☒ Set-up of mechanisms to protect against theft and limit its impacts

☐VPN is mandatory for remote access

☒ Application of ANSSI recommendations regarding protection of websites, TLS and Wi-Fi

☒ Set-up of intrusion detection systems

☒ Application of ANSSI recommendations regarding secure administration of IT systems and regarding best practice for protection of the central Active Directory

☒ Set-up of an IT business recovery and continuity plan

☒ Testing of restoration of back-ups and of application of the business recovery or continuity plan

☒ Implementation of a secure data deletion procedure

☐ Use of software programs dedicated to data deletion certified by ANSSI

☐ Others: ………………………………………………………………….

5.2. Privacy by design/Privacy by default

☒ By default and as a minimum, users configure data collection

☒ No obligation to fill in optional data fields

☒ Only data necessary for the purposes of the Data Processing are collected

☒ Automatic and selective data purge at the end of Data Processing

☒ Management of IT authorizations and access rights, looking at each piece of data, or on demand

☐ Others: ………………………………………………………………….

5.3. Data Governance

☒ Application of the 25 reference standards from Proceedings of the CNIL #2017-219 on July 13, 2017

☒ Appointment of a data protection officer

☒ Set-up of an appropriate data protection policy

☐ Others: …………………………………………………………………..

5.4. Training

☒ Regular training in GDPR principles for people participating in the Data Processing

☐ Others: …………………………………………………………………..