# USER PRIVACY AND DATA SECURITY

## 1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Data Protection Agreement (DPA). 1.1 Definitions:

| | |
|---|---|
| “Agreement” | -the agreement between the Customer and ExpensePoint including the Terms. |
| “Application” | -the SaaS (Software as a Service) based software and tools known as ExpensePoint provided by ExpensePoint including any updates ExpensePoint may make from time to time |
| “Authorized Persons“ | -the persons or categories of persons that the Customer authorizes to give ExpensePoint personal data processing instructions. |
| “Business Purposes“ | -the services described in the Agreement. |
| “Customer” | -a party to the Agreement with ExpensePoint. |
| “Customer Client” | - an internal or external client, agent, employee, customer or contractor of the Customer |
| “Customer Client Data” | -Personal Data owned and controlled by the Customer Client. |
| “Data Subject“ | -an individual who is the subject of Personal Data. |

| | |
|---|---|
| “Personal Data“ | means any information relating to an identified or identifiable natural person that is processed by ExpensePoint as a result of, or in connection with, the provision of the services under the Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| “Processing, processes and process“ | -either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes, or process. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring Personal Data to third parties. |
| “Data Protection Legislation “ | - Canada, United States, UK Data Protection Legislation, and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications). |
| “UK Data Protection Legislation “and the EU ‘Data Protection Act’ | -all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended. |
| “Personal Data Breach “ | -a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. |

| | |
|---|---|
| "Standard Contractual Clauses (SCC) " | -the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the annex to Commission Decision 2010/87/EU, where applicable a completed copy is set out at Annex 2. |
| "ExpensePoint" | GlobalPoint Technologies Incorporated dba ExpensePoint, 104 Princess Street, Winnipeg, Manitoba R3B 1K7 Canada |
| "Terms" | -the terms and conditions between ExpensePoint and Customer. |

*1.2 This DPA is subject to the terms of, and is incorporated into, the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA.*

1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes. *Note:* (applicable to UK and EU data protection).

1.4 A reference to writing or written includes email.

1.5 In the case of conflict or ambiguity between:

1.5.1 any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

1.5.2 the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail.

1.5.3 any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and

1.5.4 any of the provisions of this DPA and any executed SCC, the provisions of the executed SCC will prevail.

## 2. APPLICATION OF THIS DPA

2.1 The Customer and ExpensePoint have entered into the Agreement pursuant to which ExpensePoint provides to the Customer ExpensePoint Application for the Customer to incorporate into its business processes in order to facilitate expense reporting.

2.2 Under certain situations as described herein the Customer may require ExpensePoint to process Personal Data on behalf of the Customer.

2.3 This DPA sets out the additional terms, requirements, and conditions on which ExpensePoint will process Personal Data when providing services under the Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

## 3. PERSONAL DATA TYPES AND PROCESSING PURPOSES

3.1 The parties acknowledge that ExpensePoint's Application hosts data including Personal Data on behalf of the Customer. The Customer (or the Customer's employees, agents or anyone acting on behalf of the Customer) may give instructions through the Application to transfer Personal Data to and from third party - hosted environments. For the purposes of the Data Protection Legislation the Customer is the Data Controller and ExpensePoint and Customer are joint Data Processors. ExpensePoint is the Data Processor for Personal Data while it is hosted and processed on behalf of the Customer in the Application and the Customer is a Data Processor in so far as it provides instructions regarding the adaptation of Personal Data and the transfer of Personal Data to and from third party-hosted environments (where **Data Controller** and **Data Processor** have the meanings as defined in the Data Protection Legislation).

3.2 Without prejudice to the generality of clause 3.1, the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including ensuring that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to ExpensePoint for the duration and purposes of this Agreement so that ExpensePoint may lawfully use, process and transfer the Personal Data in accordance with this Agreement on the Customer's behalf and, without limitation, the Customer shall ensure that all Customer Clients, have been informed of, and have given and maintained their consent to permit access, monitoring, use and disclosure of all Customer Client Data by the Customer or ExpensePoint in accordance with this Agreement and for the processing instructions it gives to ExpensePoint.

3.3 Annex 1 describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which ExpensePoint may process to fulfil the Business Purposes of the Agreement.

## 4. EXPENSEPOINT'S OBLIGATIONS

4.1 ExpensePoint will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's instructions. ExpensePoint will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. In relation to Personal Data processed by ExpensePoint shall notify the Customer if, in its opinion, the Customer's instruction to process would not comply with the Data Protection Legislation. However, the Customer hereby acknowledges that where pursuant to clause 3.1 the Customer is the Data Processor in relation to instructions to transfer Personal Data into and out of the Application environment the Customer is responsible for monitoring compliance with the Data Protection Legislation.

4.2 ExpensePoint will promptly comply with any Customer request or instruction requiring ExpensePoint to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized processing.

4.3 ExpensePoint will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this DPA specifically authorizes the disclosure, or as required by law. If a law, court, regulator, or supervisory authority requires ExpensePoint to process or disclose Personal Data, ExpensePoint must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

4.4 ExpensePoint will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of ExpensePoint's processing and the information available to ExpensePoint, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4.5 ExpensePoint will promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect ExpensePoint's performance of the Agreement.

## 5. EXPENSEPOINT'S CLIENTS

5.1 ExpensePoint will ensure that all its Customer Clients:

5.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data.

5.1.2 have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

5.1.3 are aware both of ExpensePoint's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

5.2 ExpensePoint will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of ExpensePoint's clients with access to the Personal Data.

## 6. SECURITY

6.1 ExpensePoint will at all times implement appropriate technical and organizational measures against unauthorized or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex 3. ExpensePoint shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

6.1.1 the pseudonymization and encryption of personal data.

6.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

6.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

6.1.4 a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

## 7. PERSONAL DATA BREACH

7.1 ExpensePoint will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable.

7.2 ExpensePoint will immediately and without undue delay notify the Customer if it becomes aware of:

7.2.1 any accidental, unauthorized, or unlawful processing of the Personal Data; or

7.2.2 any Personal Data Breach.

7.3 Where ExpensePoint becomes aware of 7.2.1 and/or 7.2.2 above, it shall, without undue delay, also provide the Customer with the following information:

7.3.1 description of the nature of 7.2.1 and/or 7.2.2, including the categories and approximate number of both Data Subjects and Personal Data records concerned.

7.3.2 the likely consequences; and

7.3.3 description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

7.4 Immediately following any unauthorized or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter.

7.5 ExpensePoint will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.

7.6 ExpensePoint agrees that the Customer has the sole right to determine:

7.6.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

7.6.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7.7 ExpensePoint will cover all reasonable expenses associated with the performance of its obligations under clause 7.2 and clause 7.4 unless the matter arose from the Customer's specific instructions, negligence, willful default, or breach of this DPA, in which case the Customer will cover all reasonable expenses.

7.8 ExpensePoint shall only be liable for damages incurred by the Customer in relation to a Personal Data Breach where ExpensePoint's breach of its obligations under this DPA or the Data Protection Legislation has directly led to the event giving rise to the damages.

## 8. CROSS-BORDER TRANSFERS OF PERSONAL DATA OUT OF THE EEA (FOR EU CUSTOMERS)

8.1 Personal Data may be instructed to be transferred to a territory outside of the EEA by the Customer or Customer's Client's use of the Application. For the avoidance of doubt this is not a transfer by ExpensePoint and ExpensePoint has no control of such a transfer made by the Customer or Customer's Client using the Application for this purpose.

8.2 ExpensePoint shall not itself transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Customer's prior written consent.

8.3 Where such consent is granted under clause 8.2, ExpensePoint may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

8.3.1 ExpensePoint is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. ExpensePoint must identify in Annex 1 the territory that is subject to such an adequacy finding; or

8.3.2 ExpensePoint participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that ExpensePoint (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation (*(EU) 2016/679*). ExpensePoint will identify in Annex 1 the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and ExpensePoint must immediately inform the Customer of any change to that status; or

8.3.3 the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Annex 1.

## 9. SUBCONTRACTORS

9.1 ExpensePoint may only authorize a third party (subcontractor) to process the Personal Data if:

9.1.1 the Customer is provided with an opportunity to object to the appointment of each subcontractor within 30 days after ExpensePoint supplies the Customer with full details regarding such subcontractor.

9.1.2 ExpensePoint has entered into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organizational data security measures.

9.1.3 ExpensePoint maintains control over all Personal Data it entrusts to the subcontractor; and

9.1.4 the subcontractor's contract terminates automatically on termination of this DPA for any reason.

9.2 Those subcontractors approved as at the commencement of this DPA are as set out in Annex 1.

9.3 Where the subcontractor fails to fulfil its obligations under such written agreement, ExpensePoint remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

## 10. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS

10.1 ExpensePoint will, at no additional cost, take such technical and organizational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

10.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

10.1.2 information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

10.2 ExpensePoint must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

10.3 ExpensePoint must notify the Customer within 10 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

10.4 ExpensePoint will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication, or Data Subject request.

10.5 ExpensePoint must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

## 11. TERM AND TERMINATION

11.1 This DPA will remain in full force and effect so long as:

11.1.1 the Agreement remains in effect; or

11.1.2 ExpensePoint retains any Personal Data related to the Agreement in its possession or control (Term).

11.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Data will remain in full force and effect.

## 12. DATA RETURN AND DESTRUCTION

12.1 At the Customer's request, ExpensePoint will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

12.2 On termination of the Agreement for any reason or expiry of its term, ExpensePoint will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this DPA in its possession or control.

12.3 If any law, regulation, or government or regulatory body requires ExpensePoint to retain any documents or materials that ExpensePoint would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

## 13. AUDIT

13.1 At least once a year, ExpensePoint will conduct audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA.

13.2 On the Customer's written request, ExpensePoint will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as ExpensePoint's confidential

information under this DPA and the customer may be required to sign a 'Non-Disclosure Agreement' at the request of ExpensePoint.

13.3 ExpensePoint will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by ExpensePoint's management.

## ANNEX 1 PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing: to enable the Customer to provide its Clients with the Application to record expenses, attach receipts and all manner documents with relationship but not limited to corporate expenditures and business activities. To allow track mileage or kilometers driven. To all receipts to be human read and meta data extracted for the purpose of making expense entry and receipt linking easier. To download personal or corporate credit card data directly into the Application to enhance the process of organizing and creating expenses. To extract data from the Application with the purpose but not limited to uploading data into other third-party systems and creating integrations between its' own application and any other application of its' choosing using the Application and the Application tools. The functions of the Application are as described in the Agreement. Duration of Processing: for the duration of the Agreement. Nature of Processing: as determined by the Customer through their use of the Application. Business Purposes: as determined by the Customer through their use of the Application. Personal Data Categories: as determined by the Customer through their use of the Application. Data Subject Types: as determined by the Customer through their use of the Application. Authorized Persons: as determined by the Customer through their use of the Application. If relevant, ExpensePoint's legal basis for processing Personal Data outside the EEA in order to comply with cross-border transfer restrictions would be the Standard Contractual Clauses between Customer as "data exporter" and ExpensePoint as "data importer" per Annex 2. **Approved Subcontractors:** Hosting Services – Microsoft Azure Servers (Canada and USA) – Receipt Reading Processors – CloudFactory, Receipt Image Hosting – RackSpace, Data Integration Processors - Cyclr, Bank and Credit Card Transaction Integrators - Plaid, Importing Financial Credit Card Data on behalf of the Customer and Customer Clients - Visa, MasterCard and American Express as well as other Financial Institutions, Client support and issue tracking within Application and on ExpensePoint website – Jira and Drift (chat). Automated Clearing House (ACH) payments – Forte Systems

## ANNEX 2 STANDARD CONTRACTUAL CLAUSES (APPLICABLE TO UK AND EU)

Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller to processor transfers) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN

## ANNEX 3 SECURITY MEASURES

### ANNEX 3 – SECURITY MEASURES

#### PHYSICAL ACCESS CONTROLS

The application runs in secure data centers operated by Microsoft Azure Data Centers. Please see the following documents for an in-depth review of Microsoft's Data Center infrastructure, management and physical access controls. Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

#### SYSTEM & DATA ACCESS CONTROLS

Access to the application is controlled by username and password. All passwords are stored in an encrypted form. Supervisory and administrator access is restricted to authorized members of ExpensePoint Staff with permission being granted by the CTO on demonstration of a legitimate customer support or system management requirement. User access is controlled by the Customer themselves. ExpensePoint acts as a Data Processor when it comes to providing services to, and enacting the instructions of, our Direct Customers. Direct Customers are companies with a direct paid subscription to ExpensePoint application, who in turn provide expense report creation access, accounting function access, analysis reporting access and integration functionality to their own End Users (an individual, company or entity that is a client of our Direct Client). Our obligations to Customers are either covered by our online terms and conditions or an independent Enterprise Agreement depending upon the subscription and service level the Customer has with ExpensePoint. We endeavor to regularly review and update our terms and conditions and contracts and communicate any such amends in a timely fashion.

#### TRANSMISSION CONTROLS

We always encourage the use of https:// or SSL where possible when customers are connecting to ExpensePoint or third-party APIs such that data is encrypted on the way in to and out of ExpensePoint application. Whilst in ExpensePoint application environment all data is encrypted.

#### INPUT CONTROLS

The Application allows Customers and Customer Clients with the ability to directly input all manner of data including personal data into the Application via human input and via controlled API's of data transfers. The

application moves data provided through API calls – Get, Put Delete etc., inbound 'webhook' posts or FTP transfer.

## DATA BACKUPS

There are daily data backups. Backup copies of the data are made to a secure location.

## DATA SEGREGATION

Data for each client using the application is segregated in such a way that transactions being processed for one client cannot be seen by another client.

# SSAE-16 SOC1 TYPE II

ExpensePoint maintains SSAE-16 SOC1 Type II audit compliance. The report is available to current and potential customers subject to signature of appropriate Non-Disclosure Agreements.

SSAE16 is an AICPA (American Institute of Certified Public Accountants) auditing standard intended to provide customers and prospects with third party validated visibilityof a service provider's controls.

## SOC 1

- Reports are to be conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, the AICPA attest standard, which is an audit conducted over internal controls over financial reporting, management of the user organizations, and management of the service organization.

- Service Organizations continue to define their control objectives and controls, but the service auditor is responsible for evaluating those control objectives to ensure they are reasonable.

- A Type 2 report also includes the service auditor's opinion on whether the controls were operating effectively and describes tests of the controls performed by the service auditor to form that opinion and the results of those tests

## PCI-DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD)

ExpensePoint maintains PCI-DSS security standards. The Payment Card Industry Data Security Standard is a global information security standard defined by the Payment Card Industry Security Standards Council (PCI-SSC). The purpose of the standard is to reduce credit card fraud. This is achieved through increased controls around data and its exposure to compromise. The standard applies to all organizations which process, store or transmit cardholder information.

To be compliant companies must secure its network, implement secure data management policies, maintain a vulnerability management program, and implement strong access-control measures. And then you must monitor, manage, and test these policies. ExpensePoint adheres to all of these requirements.