Data Processing Agreement

1 Scope and order of precedence

1.1 **Scope.** This Data Processing Agreement, including its Appendices (1 and 2), constitutes the "**Data Processing Agreement**" or "**DPA**". The Parties have entered into an agreement related to the provision of services (the "**Agreement**"). This DPA governs each Party's obligations in relation to the Processing of personal data under the terms of the Agreement.

1.2 **Term.** This DPA shall be effective for the term of the Agreement.

1.3 **Defined terms.** For purposes of this DPA, the capitalised terms used in this DPA shall have the meaning outlined in Appendix 1 of the TOS.

2 Processing of personal data

2.1 **Purpose, Types and Categories.** The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under the scope of this DPA, and the Agreement is further defined in Appendix 1.

2.2 **Controller.** The Customer acts as the Controller in relation to any Personal Data provided by the Customer under the Agreement. The Customer is responsible for the accuracy, quality, and legality of the Personal Data and the means by which the Customer acquired the Personal Data.

2.3 **Processor.** Pagero and its Sub-processors act as the Processors of any Personal Data provided by the Customer under the Agreement and shall only process Personal Data on behalf of, and in accordance with, the Customer's lawful instructions, the Data Protection Legislation or other applicable mandatory legislation.

2.4 **Processing purposes.** The Customer shall determine the purposes of the Processing of Personal Data under the Agreement. The purposes for Processing Personal Data by Pagero and its Sub-processors are limited to:

a) fulfilling the obligations under the Agreement, such as providing a system or software, consultancy services, maintenance services, support services, expanding the Pagero network and other services to the extent agreed by the Parties under the Agreement;
b) setting up, operating, and monitoring the underlying infrastructure (hardware, software, servers, environments, connectivity, etc.) required to provide the services under the Agreement and to meet the technical, security and organisational requirements for the Processing of the Personal Data;
c) communicating to the Customer and Customer's personnel;
d) executing the Instructions of the Customer in accordance with clause 2.5 below; and
e) addressing service issues, technical problems or incidents.

2.5 **Instructions.** The Customer is responsible for issuing Instructions to Pagero regarding the processing of Personal Data under the applicable Agreement. Pagero shall only process such Personal Data in accordance with the terms of this DPA and the from time to other given Instructions provided by the Customer to Pagero. However, the Parties agree that this DPA and the Agreement set out the Customer's complete Instructions to Pagero. Changes to these Instructions shall require a separate prior written agreement between the Customer and Pagero. If Pagero considers an Instruction from the Controller to be not compliant with the Data Protection Legislation, it shall notify the Customer without undue delay.

3 Pagero Staff

3.1 **Confidentiality.** Pagero shall ensure that its and its Sub-processors' staff who have access to Personal Data are informed of the confidential nature of the Personal Data and have entered into appropriate confidentiality agreements.

3.2 **Limitation of Access.** Pagero shall ensure that Pagero's and its Sub-processors' access to the Personal Data is limited to the individuals performing services in accordance with the Agreement.

4 Protection of Personal Data

4.1 **Technical and Organisational Measures.** When Processing Personal Data on behalf of the Customer in connection with the Agreement, Pagero and its Sub-processors shall implement and maintain appropriate administrative, physical, technical and organisational security measures for the protection of the rights of

the Data Subjects in compliance with the Data Protection Legislation and in particular Article 32 GDPR. These measures shall be implemented to protect Personal Data against accidental or unauthorised loss, destruction, alteration, disclosure or access and against all other unlawful forms of Processing. Further details on the administrative, physical, technical and organisational security measures that shall be implemented and maintained by Pagero when Processing Personal Data under the Agreement are described in Appendix 2 of this DPA.

4.2 **Requests from Data Subjects or Supervisory Authority.** Pagero shall refer any contact or request from a Data Subject, a Supervisory Authority or any other third party regarding the Processing of Personal Data to the Customer. At the Customer's request, Pagero will provide the Customer with relevant information in its possession relating to the contact or request and any assistance reasonably required for the Customer to respond to the Data Subject or Supervisory Authority in a timely manner.

4.3 **Assistance.** Pagero shall assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 in the GDPR, taking into account the nature of the processing and the information available to Pagero.

5 Sub-processors

5.1 **Use of Sub-processors.** Pagero may, from time to other contract Sub-processors to meet their obligations under the Agreement. The Customer may at any time assess the current list of Sub-processors at www.Pagero.com/sub-processors (password: Compliance). Pagero shall ensure that the same data protection obligations set out in this DPA shall be imposed on the Sub-processor through a contract.

5.2 **Change of Sub-processor.** Pagero may decide to remove, replace or appoint additional Sub-processors. Pagero shall provide the Customer with a notification in writing before authorising any new Sub-processor(s) to Process Personal Data under the Agreement. If the Customer does not accept the change and/or appointment of a Sub-processor, the Customer has a right to terminate the parts of the Agreement affected by the change by notifying Pagero thereof in writing within ten (10) days of receiving the change notification, with ninety (90) days' notice.

5.3 **Additional services.** In the current list of Sub-processors, Pagero has labelled its Sub-processors depending on the service they provide. The Sub-processors labelled as "Core" may Process Personal Data on behalf of all customers. Any additional Sub-processor included or added as a result of the Customer's order of additional services shall be regarded as assessed and accepted by the Customer, including Sub-processors added at a later stage due to additions or extensions to the initial scope of the Agreement.

5.4 **Responsibility.** Pagero shall be responsible and accountable for the acts or omissions of Sub-processors to the same extent that Pagero is responsible and accountable for its own actions or omissions under this DPA.

6 Independent Data Processors

6.1 **Data Exchange.** In order to fulfil obligations under the Agreement, Pagero may, from time to other have to exchange data with Independent Data Processor(-s), for example, when sending or receiving invoice data to/from other service providers.

6.2 **Pagero responsibility.** Pagero can under no circumstance be held responsible for any such Independent Data Processor's Processing of Personal Data.

7 Audit rights

7.1 **Audits.** The Customer is entitled to audit Pagero's Processing under the Agreement to ensure compliance with this DPA, subject to the provisions below. Pagero shall always allow for and cooperate with; any audits conducted or required by a Supervisory Authority responsible for monitoring the Customers' Processing of Personal Data.

7.2 **Customer Audits.** Pagero shall provide the Customer or the Customer's independent third-party auditor with such information and documentation as may reasonably be required to satisfy that Pagero is complying with the obligations referred to in this DPA. Before such audits, the Customer shall provide Pagero with reasonable written notice (at least 30 days unless a Supervisory Authority requires the Customer's earlier control under mandatory laws).

7.3 **Customer Audit Restrictions.** The following audit restrictions shall apply:

a) Unless required by the Data Protection Legislation or if the Customer has a reason to suspect that Pagero or a Sub-processor is not complying with the obligations referred to in this DPA, an audit pursuant to clause 7.2 is limited to once in any twelve-month period.
b) The Customer shall conduct the audit within a reasonable time, with reasonable conditions, during regular business hours and subject to Pagero's security policies. An audit may not unreasonably interfere with Pagero's business activities.
c) Each party shall be responsible for their respective costs in relation to an audit under this DPA.

7.4 **Audit Findings.** Without prejudice to any other of the Customers rights or remedies, Pagero shall without unreasonable delay effect a remedy if an audit determines that Pagero or a Sub-processor has breached its obligations under this DPA. If Pagero cannot remedy an audit remark, Pagero must notify the Customer. The Customer is then entitled to terminate the Agreement without any compensation.

8 Incident management and security breach notification

8.1 **Incident management.** Pagero shall evaluate and respond to events suspected to lead to unauthorised access to or handling of Personal Data ("**Incidents**"). If there is a risk that the Incident may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, Pagero will notify the Customer without undue delay after becoming aware of a personal data breach and provide relevant information regarding the Incident. Pagero will define appropriate activities to address Incidents and work with the Customer when appropriate to protect the Personal Data. The objective of the Incident response will be to restore the confidentiality, integrity, and availability of the related service and Personal Data. The Customer is responsible for registering a point of contact within the Software Services as the designated point of contact in case of incidents and to keep this information up to date.

9 Return and deletion of Customer data

9.1 **Return and deletion.** Pagero shall, upon the Customers' request, return all stored Personal Data provided by the Customer under the scope of the Agreement to the Customer and then delete all such data within ninety (90) days (an additional thirty (30) days in backups) after the termination of the Agreement or this DPA, unless otherwise agreed in writing. Due to the different nature of such files, payment instructions will be deleted after twenty-four (24) months. For the avoidance of doubt, all Personal Data is deleted on an ongoing basis.

10 Transfer of personal data

10.1 **General.** Pagero and its Sub-processors shall not Process or transfer Personal Data outside of the EU, or the EU Approved Countries without a written mandate from the Customer.

10.2 **Transfers.** Pagero may transfer Personal Data to approved Sub-processors located in a country or territory outside of the EEA, or the EU Approved Countries, and to allow such Sub-processors to access and process Personal Data from a country or territory located outside of the EEA or the EU Approved Countries, solely for the purposes stated in clause 2.4, and if:
a) the transfer is governed by and in accordance with a suitable framework recognised by the relevant authorities or courts as providing an adequate level of protection for personal data, including without limitation Binding Corporate Rules for Processors; or
b) the transfer is governed by and in accordance with the Standard Contractual Clauses issued by the European Commission in accordance with article 46(c). In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. For the avoidance of doubt, the Standard Contractual Clauses will only apply to transfers of Personal Data, or
c) any other approved means of transfer under articles 46 or 49.

DPA Appendix 1

1. Roles

In the handling of Personal Data, the Parties acknowledge that:

- The Customer will act as Controller and Pagero as Processor in respect of Personal Data processed in e-Documents within the Software Services.
- The Customer will act as Controller for the administration and management of the Customer's User Accounts within the Software Services.
- Pagero will act as the Controller when processing Personal Data relating to Customer contacts, such as contact information, in order to administer the business relationship with the Customer.

2. Data Subjects

The Processing of Personal Data covered by this DPA concerns the following categories of Data Subjects:

Pagero will only process Personal Data on Data Subjects as provided by the Customer, typically including but not limited to:

- Employees/ personnel of the Customer.
- References/contacts of business partners.

3. Categories of Personal Data

The processed personal data concerns the following categories of data (please specify):

Pagero will only process Personal Data on Data Subjects as provided by the Customer, typically including but not limited to:

- Contact details (name, email, phone).
- Any Personal Data as may be included in the business documents, including Personal Data derived from goods or services ordered, bought or sold.

4. Special categories of Personal Data (if appropriate)

The processed personal data concerns the following special categories of data (please specify):

Depending on the documents processed in the service by the Customer, personal data relating to health, sex, political opinion or religion may indirectly be processed, e.g., if the services are used to send invoices for hospital visits or similar.

5. Processing activities

The Processed Personal Data will be subject to the following basic processing activities):

The Personal Data will be Processed within the framework of the provision and operation of the Software Services and any value-added services. The system will be available to the Customer in its daily operations and for Pagero to provide support and maintenance. The Personal Data will be stored and Processed, for example, in different e-Documents, including but not limited to orders and invoices.

6. List of Sub-processors

The Processing of Personal Data covered by this DPA may be performed by one or several of Pagero's Sub-processors. By agreeing to the terms of this DPA, Customer approves Pagero's current list of Subprocessors (as applicable in accordance with clause 5.3 of the DPA):

The current list of Sub-processors can be found here under www.Pagero.com/sub-processors

For the avoidance of doubt, all Sub-Processors listed as “Core” apply to all Customers; other listed Sub-Processors are applicable depending on the add-on services ordered by the Customer, such as, e.g., print, scanning or data capture services.

To access the list, please enter the password: Compliance (this link may not be disclosed to unauthorised external parties)

DPA Appendix 2

Description of the technical and organisational security measures to be implemented for the protection of Personal Data.

The purpose of this document is to describe the technical and organisational measures in place within all services that Pagero offers to our customers to ensure the appropriate protection of personal data.

1. Risk assessment regarding data protection

Pagero conducts a documented risk assessment for the services provided to our customers. The risk assessment is reviewed regularly, and any findings based on the risk assessment are evaluated, documented, and managed in order to fulfil the legal requirements.

The risk assessment process is built around five different steps;

- Identify risk
- Analyse and assess risk
- Perform decision making
- Implement decision
- Validate the effectiveness of the decision

2. Security measures

As a part of our information security management system (ISMS), Pagero has made a part of the documentation available upon request for our customers. The documentation that is available is classified as public or restricted information. All documentation within Pagero ISMS is reviewed regularly as a part of our ISAE audit program and our Cyber Essential certification. The ISAE audit is performed by an independent auditor and is based upon the trust service principles of Confidentiality, Integrity and Availability. The ISAE audit report is available upon request for our customers and prospects.

3. Roles and responsibilities

Pagero has established internal roles to ensure the appropriate protection of personal data. Pagero has a CISO responsible for developing, managing and auditing Pagero's ISMS and has appointed a Data Protection Officer who oversees Pagero's data protection practices and reports directly to the board of directors.

4. Pseudonymisation and encryption of personal data

Pagero uses pseudonymisation and/or encryption where possible to protect the personal data of customers and reduce the risk of data exposure. The security measures vary between different services and products depending on risk level, technical solution, and type of product.

- All data at rest is encrypted
- Passwords are hashed and stored in an encrypted form
- If personal data are used in a test environment, the data is pseudonymised according to company policy and routines.
- Backup files are stored in encrypted form in an offsite location according to company policy.

5. Confidentiality, Integrity and Availability

Multiple security controls are in place to secure that a person only can access the data they are authorised to view, and Pagero performs reviews on access rights and accounts regularly.

- Pagero manages access to customer data in the following ways:
    - Pagero has strict controls around accounts and account creation:
    - Accounts may be granted only to individuals with a verified business need.
    - Accounts are never to be shared with anyone for any reason.

- Accounts must be granted with the minimum level of access and on the minimum number of systems required for the user to complete their required business tasks.
- Accounts must only be issued when authorisation for the accounts can be verified.
- Abuse of accounts results in immediate account termination.
- Account credentials must meet the password complexity requirements for Pagero.
- Accounts determined to be idle or unused by otherwise active employees, contractors, or consultants for a period of six months must be disabled, and the direct supervisor of the account holder notified.

6. Data centres

Only authorised staff with valid business reasons have access to our data centres. The data is protected from accidental or illegal destruction or loss by physical and environmental controls. The physical and environmental controls are reviewed on a yearly basis as a part of our ISAE audit report. Remote access to our data centres is secured by 2-factor authentication.

- Pagero has taken the following measures to ensure entry control in order to prevent unauthorised parties from being able to enter data processing systems:
  - Network security
    - The network is divided into different subnets
    - IDS and IPS are in place
    - Firewalls are in place, and the settings are reviewed on a regular basis in accordance with company policies
  - Pagero enforces the use of complex passwords or biometric identification in combination with a 2-step login process in accordance with our company policy.
- Pagero ensures the physical security of access to customer data in the following ways:
  - All data centres are ISO 27001 certified, audited in accordance with the ISAE audit standard or have a similar level of equivalent security framework.
  - Sensitive areas and systems must be physically secured, and access permitted only to authorised individuals, all of whom must demonstrate that they understand Pagero security policies. Access to sensitive areas is logged.
  - Access is revoked upon inappropriate use, security breach, or employee termination.
  - Servers are physically located in an access-controlled environment
- Pagero Ensures that data is protected from accidental or illegal destruction in the following ways
  - Backups are stored outside the data centre
  - Warm standby environment where data is transferred regularly in accordance with company policies
  - The data centres are protected against environmental incidents in accordance with industrial standards
  - Redundant power systems (UPS for example)
  - Protected against flooding
  - Fire alarm/protection

7. Pagero Online

Pagero Online and our other cloud services are hosted in a private cloud. Only authorised staff within the Pagero Group have access to the environment, and a 2-factor login process is mandatory for these user groups. The data is protected from accidental or illegal destruction by physical and environmental controls. The physical and environmental controls are reviewed on a yearly basis as a part of our ISAE audit report.

- The cloud service is built upon two independent data centres where one of the data centres is a “warm” standby data centre as described in clause 6 “data centre” above”
- The data is backed-up according to industry standards and is protected from accidental or illegal destruction by physical and environmental controls as described in clause 6 “data centre” above”
- The backup process is tested on a regular basis in order to secure that it is possible to restore the data in an effective manner.

8. Internal system within Pagero Group

Internal systems within the Pagero Group are only accessible via our secure intranet solution, and access to our intranet is protected by a 2-factor VPN solution in order to secure that only approved internal or external personnel can access the systems.

External Pagero tools hosted in the cloud outside Pagero intranet are protected by one or several of the following standards; Active Directory Federation Services (AD FS), 2-factor login, approved IP ranges, username and password handling. Each external system is reviewed in accordance with the supplier management routine and a risk management routine to set the security level of the application. Criteria that are included in the risk process is

- Type of data stored (internal data, customer data)
- Place of storage
- Number of employees accessing the application

All internal systems that contain customer data are always protected by either VPN or 2-factor login.

9. Business Continuity

To secure system availability and access to personal data in the event of technical or physical incidents, Pagero has backup processes in place and also independent secondary warm standby data centres to secure access to personal data in our cloud services.

Pagero has defined how business continuity should be achieved in the event of a critical system failure to provide our customers with high availability to the cloud services. The business continuity plan is tested on a regular basis in order to minimise manual steps and to make the plan as effective as possible. The business continuity plan is reviewed on a yearly basis by an independent auditor as a part of our ISAE audit report.