

**Data processing agreement**

**behandleraftale**

Data Processing Agreement

by and between

|  |  |
| --- | --- |
| **Data Controller:** | [Customer] |
| Organisation number: | [VAT NR] |
| Country of establishment: | [Country] |
| Data Controller’s contact for general requests regarding the agreement (name, role, contact details): | [Name] |
| Data Controller’s contact for notification of unauthorised data processing (name, role, contact details):  | [E-mail address] |
|  |  |
| **Data Processor:** | pensopay A/S |
| Organisation number: | 36410876 |
| Country of establishment: | Denmark  |
| Data Processor’s contact for general requests regarding the agreement (name, role, contact details): | Pierre Rindsig, CEO |
| Data Processor’s contact for notification of unauthorised data processing (name, role, contact details): | pr@pensopay.com |

Henceforth respectively referred to as “Controller”, “Processor”, or “Party” and collectively as the “Parties”.

#

# Introduction

1.1. Both Parties confirm that the undersigned have the power of attorney to enter into this data processing agreement (“Agreement”). This Agreement will form part of and regulate the processing of personal data tied to the following service agreements ("Service Agreements") between the Parties:

* Agreement regarding payment solution

1.2. If the Controller changes the contact person(s) mentioned in the table above, the Processor must be informed of this in writing.

1.3 This agreement regarding the processing of personal data (the "Data processing agreement") regulates Pensopay APS CVR no. 36410876 (the data processor) and the Customer (the "Data Controller") and is an appendix to the general conditions. The Data Controller and the Data Processor are hereafter referred to collectively as "Parties" and individually as "Party".

1.4 The Data Controller and the Data Processor have entered into an agreement regarding a payment solution including payment gateway and acquiring (“the Agreement”).

1.5. As part of the Data Processor's delivery of the Services (as defined below) to the Data Controller in accordance with the Agreement, the Data Processor must process personal data on behalf of the Data Controller.

1.6 Applicable Data Protection Legislation (as defined below) requires that a written contract be entered into between a data controller and a data processor who processes personal data on behalf of the data controller, which determines the scope of and the requirements for the processing in question. The parties have therefore entered into this Data Processor Agreement (as defined below).

# Definitions

2.1. The definition of Personal Data, Special Categories of Personal Data (Sensitive Personal Data), Processing of Personal Data, Data Subject, Controller and Processor is equivalent to how the terms are used and interpreted in applicable privacy legislation, including the EU 2016/679 General Data Protection Regulation (“GDPR”).

2.2 Unless otherwise indicated in the context, the following terms have the following meanings:

1. The "agreement" has the meaning in section 1.1 stated meaning.

2. "Data processing agreement" means this agreement on the processing of personal data, including annexes.

3. "Data protection legislation" means all the laws and regulations that apply to the processing and protection of personal data throughout the European Economic Area (EEA) with the amendments and/or additions applicable at any time, including directive 95/46/EC of 24 October 1995 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data, the Personal Data Act (as defined below), the Ordinance on Data Protection (as defined below) and, where relevant, the guidelines and regulations issued by the EEA and/or other relevant national authorities in the EEA (including the national data supervisors).

4. "Regulation on Data Protection" means "Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of directive 95/46/EC (general data protection regulation)" with the amendments and/or additions applicable at any time.

5. "The Personal Data Act" means Act No. 429 of 31 May 2000 on the processing of personal data with the amendments and/or additions applicable at any time.

6. "The Services" means the services and supplies that the Data Processor as supplier provides to the Data Controller as customer in accordance with the Agreement.

2.3 The terms "personal data", "special categories of personal data", "processing", "data controller", "data processor", "registered", "supervisory authority", "pseudonymisation", "technical and organizational measures" and "breach of personal data security" this Data Processor Agreement is understood to be in accordance with applicable Data Protection legislation, including the Ordinance on Data Protection.

1. Scope

3.1. The Agreement regulates the Processor's Processing of Personal Data on behalf of the Controller, and outlines how the Processor shall contribute to ensure privacy on behalf of the Controller and its registered Data Subjects, through technical and organisational measures according to applicable privacy legislation, including the GDPR.

3.2. The purpose behind the Processor’s Processing of Personal Data on behalf of the Controller is to fulfill the Service Agreement(s).

3.3. This Agreement takes precedence over any conflicting provisions regarding the Processing of Personal Data in the Service Agreements or in other former agreements or written communication between the Parties. This Agreement is valid for as long as agreed in Appendix A.

# The Processor’s rights and obligations

4.1. The Processor shall only Process Personal Data on behalf of and in accordance with the Controller’s written instructions. By entering into this Agreement, the Controller instructs the Processor to process Personal Data in the following manner; i) only in accordance with applicable law, ii) to fulfill all obligations according to the Service Agreement, iii) as further specified via the Controller’s ordinary use of the Processor’s services and iv) as specified in this Agreement.

4.2. The Processor has no reason to believe that legislation applicable to it prevents the Processor from fulfilling the instructions mentioned above. The Processor shall, upon becoming aware of it, notify the Controller of instructions or other Processing activities by the Controller which in the opinion of the Processor, infringes applicable privacy legislation.

4.3. The categories of Data Subject’s and Personal Data subject to Processing according to this Agreement are outlined in Appendix A.

4.4. The Processor shall ensure the confidentiality, integrity and availability of Personal Data are according to the privacy legislation applicable to The Processor. The Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, taking into account the state of the art and cost of implementation in relation to the risk represented by the Processing, and the nature of the Personal Data to be protected.

4.5. The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible and taking into account the nature of the Processing and the information available to the Processor, in fulfilling the Controller’s obligations under applicable privacy legislation with regards to request from Data Subjects, and general privacy compliance under the GDPR article 32 to 36.

4.6. If the Controller requires information or assistance regarding security measures, documentation or other forms of information regarding how the Processor processes Personal Data, and such requests exceed the standard information provided by the Processor to comply with applicable privacy legislation as Processor, the Processor may charge the Controller for such request for additional services.

4.7. The Processor and its staff shall ensure confidentiality concerning the Personal Data subject to Processing in accordance with the Agreement. This provision also applies after the termination of the Agreement.

4.8. The Processor will, by notifying the Controller without undue delay, enable the Controller to comply with the legal requirements regarding notification to data authorities or Data Subjects about privacy incidents.

Further, the Processor will to the extent it is appropriate and lawful notify the Controller of;

i) requests for the disclosure of Personal Data received from a Data Subject,

ii) requests for the disclosure of Personal Data by governmental authorities, such as the police

4.9. The Processor shall ensure that persons that have the right to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.10. The Processor will not respond directly to requests from Data Subjects unless authorised by the Controller to do so. The Processor will not disclose information tied to this Agreement to governmental authorities such as the police, hereunder Personal Data, except as obligated by law, such as through a court order or similar warrant.

4.11. The Processor does not control if and how the Controller uses third party integrations through the Processor's API or similar, and thus the Processor has no ownership to risk in this regard. The Controller is solely responsible for third party integrations.

4.12. The Processor might Process Personal data about users and the Controllers use of the service when it is necessary to obtain feedback and improve the service. The Controller grants the Processor the right to use and analyze aggregated system activity data associated with your use of the Services for the purposes of optimizing, improving or enhancing the way the Processor provides the services and to enable the Processor to create new features and functionality in connection with the services. Visma shall be considered the Controller for such processing and the processing is therefore not subject to this Agreement.

4.13. When using the service, the Controller will add data to the Software (“Customer Data”). The Controller acknowledges and does not object to the Processor using Customer Data in an aggregated and anonymized format for improving the services delivered to customers, research, training, educational and/or statistical purposes.

# The Controller’s rights and obligations

Regardless of the provisions of this Agreement, the Data Processor has the right to process personal data without instructions from the Data Controller, if and to the extent required by other EU law and/or the national law of the Member States. In that case, however, the Data Processor must first, to the extent that it is legal, notify the Data Controller of such an order and, to the extent possible, give the Data Controller the opportunity to object to this.

5.1. The Controller confirms by the signing of this Agreement that:

* The Controller has legal authority to process and disclose to the Processor (including any subprocessors used by the Processor) the Personal Data in question.
* The Controller has the responsibility for the accuracy, integrity, content, reliability and lawfulness of the Personal Data disclosed to the Processor.
* The Controller has fulfilled its duties to provide relevant information to Data Subjects and authorities regarding processing of Personal Data according to mandatory data protection legislation.
* The Controller shall, when using the services provided by the Processor under the Services Agreement, not communicate any Sensitive Personal Data to the Processor, unless this is explicitly agreed in Appendix A to this Agreement.

# Use of subprocessors and transfer of data

6.1. As part of the delivery of services to the Controller according to the Service Agreements and this Agreement, the Processor will make use of subprocessors and the Controller gives its general consent to usage of subprocessors. Such subprocessors can be other companies within the Visma group or external third party subprocessors. All subprocessors are included in Appendix B. The Processor shall ensure that subprocessors agree to undertake responsibilities corresponding to the obligations set out in this Agreement.

6.2. An overview of the current subprocessors with access to Personal Data can be found in the Visma Trust Centre on this web site: <https://www.visma.com/trust-centre/product-search/>. The Processor may engage other EU/EEA located companies in the Visma Group as subprocessors without the Visma company being listed at Trust Center and without prior approval or notification to the Controller. This is usually for the purposes of development, support, operations etc. The Controller may request more detailed information about subprocessors.

6.3. If the subprocessors are located outside the EU or the EEA, the Controller gives the Processor authorisation to ensure proper legal grounds for the transfer of Personal Data out of the EU /EEA on behalf of the Controller, hereunder by entering into EU Standard Contractual Clauses (SCCs).

6.4. The Controller shall be notified in advance of any changes of subprocessors that Process Personal Data. If the Controller objects to a new subprocessor within 30 days after a notification is given, the Processor and Controller shall review the documentation of the subprocessors compliance efforts in order to ensure fulfillment of applicable privacy legislation. If the Controller still objects and has reasonable grounds for this, the Controller can not reserve themselves against the use of such a subprocessor (due to the nature of online standard Software in particular), but the Customer may terminate the Service Agreement for which the subprocessor in dispute is being used for.

# Security

7.1. The Processor is committed to provide a high level of security in its products and services. The Processor provides its security level through organisational, technical and physical security measures, according to the requirements on information security measures outlined in the GDPR article 32.

7.2. The Service Agreement sets forth the measures or other data security procedures that the Processor implements in the Processing of the Personal Data. The Controller shall be responsible for the appropriate and adequate security of the equipment and the IT environment under its responsibility. When assessing which level of security is appropriate, the Data Processor must in particular take into account the risks associated with the processing, including but not limited to the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data that is transmitted, stored or otherwise processed.

7.3. The Data Processor must also meet any security requirements that are incumbent on the Data Processor in accordance with applicable Data Protection legislation, including applicable security requirements in the country in which the Data Processor is established.

7.4. The Data Processor shall, by means of appropriate technical and organizational measures, assist the Data Controller in fulfilling the Data Controller's obligation to respond to requests for the exercise of data subjects' rights in accordance with applicable Data Protection legislation.

7.5. The data processor must notify the Data Controller without undue delay after becoming aware that there has been a breach of personal data security. Furthermore, the Data Processor must assist the Data Controller in ensuring compliance with the Data Controller's obligations to (i) document all breaches of personal data security, (ii) report any breaches of personal data security to the competent supervisory authority(ies) and (iii) notify the registered about such breaches of personal data security, all in accordance with Articles 33 and 34 of the Data Protection Regulation.

# Audit rights

8.1. The Controller may audit the Processor’s compliance with this Agreement up to once a year. If required by legislation applicable to the Controller, the Controller may request audits more frequently. To request an audit, the Controller must submit a detailed audit plan at least four weeks in advance of the proposed audit date to the Processor, describing the proposed scope, duration, and start date of the audit. If any third party is to conduct the audit, it must as a main rule be mutually agreed between the Parties. However, if the processing environment is a multitenant environment or similar, the Controller gives the Processor authority to decide, due to security reasons, that audits shall be performed by a neutral third party auditor of the Processor’s choosing.

8.2. If the requested audit scope is addressed in an ISAE, ISO or similar assurance report performed by a qualified third party auditor within the prior twelve months, and the Processor confirms that there are no known material changes in the measures audited, the Controller agrees to accept those findings instead of requesting a new audit of the measures covered by the report.

8.3. In any case, audits must be conducted during regular business hours at the applicable facility, subject to the Processors policies, and may not unreasonably interfere with the Processors business activities.

8.4. The Controller shall be responsible for any costs arising from the Controller’s requested audits. Requests for assistance from the Processor may be subject to fees.

# Term and termination

9.1. This Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller after the Service Agreements or as otherwise agreed in Appendix A.

9.2. This Agreement is automatically terminated upon termination of the Service Agreement. Upon termination of this Agreement, the Processor will delete or return Personal Data processed on behalf of the Controller, according to the applicable clauses in the Service Agreement. Such deletion will take place as soon as reasonably practicable, unless EU or local law requires further storage. Unless otherwise agreed in writing, the cost of such actions shall be based on; i) hourly rates for the time spent by the Processor and ii) the complexity of the requested process.

# Changes and amendments

10.1. Changes to the Agreement shall be included in a new Appendix to this Agreement and signed by both Parties in order to be valid.

10.2. If any provisions in this Agreement become void, this shall not affect the remaining provisions. The Parties shall replace the void provision with a lawful provision that reflects the purpose of the void provision.

# Liability

11.1. For the avoidance of doubt, the Parties agree and acknowledge that each Party shall be liable for and held accountable to pay administrative fines and damages directly to data subjects which the Party has been imposed to pay by the data protection authorities or authorized courts according to applicable privacy legislation. Liability matters between the Parties shall be governed by the liability clauses in the Service Agreement between the Parties.

11.2. The parties' liability for all cumulative claims under this Data Processor Agreement is limited to the total due payments under the Main Services for the 12-month period immediately preceding any damaging circumstance. If the Data Processing Agreement has not been in force for 12 months, the amount is calculated proportionally on the basis of the agreed payment during the period that the Data Processing Agreement has been in force.

11.3. The limitation of liability does not include the following: (i) Losses resulting from the grossly negligent or willful actions of the other Party. (ii) Expenses and resource consumption when fulfilling a Party's obligations towards a supervisory authority.

# Governing law and legal venue

12.1. This Agreement is subject to the governing law and legal venue as set out in the Service Agreement between the parties.

1. **Transfer of personal data to a third country or an international organisation**

The data processor may not transfer personal data outside the EEA or access personal data outside the EEA without prior written consent from the data controller. If the Data Controller gives such consent, the Data Processor is obliged to ensure that (i) such a transfer is legal, including that there is a sufficient level of protection for the transfer of personal data, e.g. when entering into the standard contractual provisions for the transfer of personal data to data processors established in countries outside the EEA, pursuant to the Commission's decision of 5 February 2010 (or any subsequent decision replacing the earlier one) between, on the one hand, the data controller and on the other hand, the Data Processor and any sub-processors, (ii) all necessary approvals have been obtained, and (iii) all necessary notifications regarding the relevant transfer have been given to the relevant supervisory authority.

1. **General obligations of the data processor**

14.1 The Data Processor must apply and comply with applicable Data Protection legislation and must not perform its obligations under the Agreement in a way that may contribute to the Data Controller breaching its obligations under applicable Data Protection legislation, including by e.g. without prior notice to introduce new technologies which would have required the Data Controller to carry out an impact assessment pursuant to Article 35 (Data Protection Impact Assessments) of the Data Protection Regulation and, where applicable, prior consultation with the supervisory authority pursuant to Article 36 ( Prior consultation) in the Ordinance on Data Protection prior to processing.

14.2. The Data Processor further guarantees that it will assist the Data Controller in complying with the Data Controller's obligations under applicable Data Protection legislation, including in relation to Article 35 (Impact analyzes regarding data protection) and Article 36 (Prior consultation) of the Ordinance on Data Protection.

14.3. The data processor must, and must ensure that its sub-data processors, cooperate in an open and constructive manner with the Data Controller, the Data Controller's external auditors and the supervisory authorities, including by

a) to make all information regarding the delivery of the Services available to the Data Controller and any supervisory authority and/or the Data Controller's external auditors, if this is necessary for the performance of their tasks; and

b) to grant access to any supervisory authority that is entitled by law to access the facilities of the Data Controller or the facilities of the Data Controller's suppliers to such facilities.

# Appendix A - Data subjects, Types of personal data, Purpose, Nature, Duration

**A.1 Categories of Data Subjects**

* customer end users
* customer employees
* customer contact persons

**A.2 Categories of Personal Data**

* contact information such as name, phone, address, e-mail.
* In accordance with AML pictureID and AddressID is viewed. The mentioned are only stored encrypted until the time af activation of agreement.

**A.3 Special categories of Personal Data (Sensitive Personal Data)**

None of following types of Sensitive Personal Data is handled.

|  |
| --- |
| racial or ethnic origin, or political, philosophical or religious beliefs, |
| health information, |
| sexual orientation, |
| trade union membership |
| genetic or biometric data |

**A.4 Purpose of the processing**

The purpose of the data processor’s processing of personal data on behalf of the data controller is to deliver a payment solution. Payment card information is handled encrypted from the card holder to the card issuer, and thus not accessible for 3rd parties.

**Appendix B - Overview of subprocessors**

The subprocessors of the Processor with access to the Controller’s Personal Data upon signing this Agreement can be seen here: <https://pensopay.com/en/privacypolicy/>

The Processor may engage other EU/EEA located companies in the Visma Group as subprocessors without the Visma company being listed above and without prior approval or notification to the Controller. This is usually for the purposes of development, support, operations etc.