Appendix 11 - Data Processing Agreement

Visma Time

Visma Enterprise A/S

1. Table of Contents

2. Introduction

In connection with the Parties' Agreement, the following Data Processing Agreement shall apply from the signature date between the Data Processor, Visma Enterprise A/S, and the Data Controller, the Customer, unless otherwise expressly stated in other agreements between the parties.

The purpose of the Data Processing Agreement is to regulate how and for which purpose the Processor will process Personal Data on behalf of the Controller and to ensure that the Controller's Personal Data are processed in accordance with the guidelines and instructions of the Controller as well as the current data protection legislation.

Categories of Data Subjects and Personal Data processed are stated in Appendix A.

This Data Processing Agreement shall only apply to the product Visma Time.

3. Definitions

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 General Data Protection Regulation (GDPR) applicable for this Agreement and Europe from 25 May 2018.

4. Scope

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.

The purpose behind the Processor's Processing of Personal Data on behalf of the Controller is to fulfil the Service Agreements and this Agreement.

This Agreement takes precedence over any conflicting provisions regarding the Processing of Personal Data in the Service Agreements or in other agreements made between the Parties. This Agreement is valid for as long as the Parties have a valid Service Agreement which includes Processing of Personal Data.

5. Data Controller's obligations

The Controller confirms by the signing of this Agreement that:

- The Controller shall, when using the services provided by the Processor under the Services Agreements, process Personal Data in accordance with the requirements of applicable privacy legislation.
- The Controller has legal authority to process and disclose to the Processor (including any subcontractors used by the Processor) the Personal Data in question.
- The Controller has the sole responsibility for the accuracy, integrity, content, reliability and lawfulness of the Personal Data disclosed to the Processor.

- The Controller has fulfilled all mandatory requirements and duties to file notifications with or get authorisation from the relevant regulatory authorities regarding the processing of the Personal Data.
- The Controller has fulfilled its duties to provide relevant information to Data Subjects regarding processing of Personal Data according to mandatory data protection legislation.
- The Controller agrees to that the Processor has provided guarantees with regards to implementation of technical and organisational security measures sufficient to safeguard Data Subject's privacy rights and their Personal Data.
- 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.
- The Controller shall maintain an up to date register over the types and categories of Personal data it Processes, to the extent such Processing deviates from categories and types of Personal Data included in Appendix A.

6. Data Processor's obligations

The Processor processes only Personal Data on behalf of and on the basis of instructions from the Controller.

Data processing shall take place in the following way:

- solely in accordance with the applicable legislation,
- to fulfil all obligations under the Agreement,
- as detailed by the Controller's ordinary use of the Processor's services,
- as stated in this Data Processing Agreement.

The Processor shall notify the Controller immediately if, in the Processor's opinion, an instruction is in contravention of the General Data Protection Legislation or data protection provisions in other EU legislation or the national legislation of the member states.

The Processor shall ensure that Personal Data is subject to confidentiality, integrity and accessibility in accordance with the applicable legislation on the processing of personal data.

The Processor and its employees shall ensure confidentiality with respect to the Personal Data processed. This provision shall also apply after the termination of the Agreement.

The Data Processor shall ensure that persons authorised to process Personal Data on behalf of the Controller are bound by confidentiality or subject to appropriate statutory secrecy.

The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests from the Data Subject and on the general exercise of the Data Subject's rights laid down in Chapter III and Articles 32-36 in the General Data Protection Regulation.

The Processor shall, without undue delay, notify the Controller of incidents which the Controller is obliged by law to notify to the Danish Data Protection Agency or Data Subjects.
In addition, the Processor shall notify the Controller of the following if deemed appropriate and lawful:

- Requests for disclosure of Personal Data received from a Data Subject.
- Requests for disclosure of Personal Data from public authorities such as the police.

The Processor does not reply to direct enquiries from Data Subjects unless the Controller has given consent. The Processor does not disclose Personal Data to public authorities such as the police unless there is a legal basis for this.

The Processor has neither ownership nor control of whether and how the Controller chooses to use any third party integrations through the Processor's API via direct database connection or the like. Responsibility for such integrations with third parties rests only with the Controller.

7. Security

The Processor shall implement systematic, organisational and technical measures to ensure a suitable level of security with due consideration for technology and the costs of implementation in relation to the risks involved in the processing and the nature of the Personal Data to be used.

The Processor shall ensure a high level of security in its products and services. The Processor shall provide this level of security through organisational, technical and physical security measures in accordance with the requirements for information security measures stated in article 32 of the General Data Processing Regulation.
Furthermore, the purpose of the internal framework for the protection of personal data prepared by the Visma group is to ensure confidentiality, integrity, security and accessibility of Personal Data. The following measures are particularly important in this connection:

- Classification of Personal Data to ensure implementation of security measures corresponding to risk assessments.
- Assessment of the use of encryption and anonymization as risk-limiting measures.
- Restriction of access to Personal Data to those who need access in order to fulfil obligations under the Agreement.
- Control systems that register, restore, prevent and report breaches in connection with the processing of Personal Data.

If the Controller requests information on security measures, documentation or other forms of information on how the Controller processes Personal Data, and this information exceeds the standard information made available by the Processor for the observance of the current legislation on the processing of personal data as a processor, and this results in additional work for the Processor, the Processor shall be entitled to request payment from the Controller for such additional work.

The Processor shall notify the Controller without undue delay after having become aware of a breach of personal data security at the Processor or any sub-processor.

8. Audit

The Controller may carry out an audit up to once a year to ensure that the Processor observes this Agreement. If it is a statutory requirement applicable to the Controller, the Controller may request more frequent audits.

To make a request for the performance of an audit, the Controller shall submit a detailed audit plan at least four (4) weeks prior to the suggested audit date to the Processor with a description of the suggested scope, duration and start date of the audit.

If an inspection is to be carried out by a third party this must, as a main rule, be agreed between the Parties. If processing takes place in a multi-tenant environment or the like the Controller entitles the Processor to decide, for security reasons, that the inspections are carried out by a neutral third party inspector appointed by the Processor.
If the requested scope of the inspection is described in ISAE, ISO or similar security report handled by a qualified third party inspector within the last 12 months, and the Processor confirms that no significant changes have been made to the measures inspected, the Controller shall confirm that such results are accepted instead of requesting a new inspection of the measures comprised by the report.
In any case, inspections shall be carried out within normal working hours at the site in pursuance of the Processor's policies and shall not unreasonably interfere with the Processor's business operations.
The Controller shall pay all costs in connection with audits or inspections requested by the Controller.
The Processor shall also invoice the Controller for assistance in excess of the standard service made available by the Processor or the Visma group for the observance of the relevant legislation on the processing of personal data.

9. Use of sub-processors and transfer of data

As part of the delivery of services to the Controller, the Processor shall have general authorization from the Controller to use sub-processors. These sub-processors may be other companies in the Visma group or external third party suppliers.

The Processor shall ensure that sub-processors are subject to the same obligations as those stipulated in this Data Processing Agreement. Any use of sub-processors shall be subject to the Visma group's Privacy Statement.

The Controller shall be entitled to request an overview of sub-processors currently used with access to personal data as stated in Annex B. The Controller shall also be entitled to request a full overview and more detailed information on these sub-processors.

The Controller shall be notified in advance of any replacement of sub-processors processing Personal Data. The Controller may object to the changes if the Controller has reasonable and specific reasons for this.

The Processor must not permit the processing of Personal Data outside the EU/EEA without the Controller's consent.

If the Controller consents to the Processor processing Personal Data outside the EU/EEA this is stated in Appendix B. The Processor shall ensure a correct legal basis for the transfer of Personal Data outside the EU/EEA on behalf of the Controller.

10. Duration and termination

This Data Processing Agreement shall remain effective as long as the Processor processes Personal Data on behalf of the Controller under the Agreement.
Upon termination of this Agreement, the Processor shall erase, return or store the Personal Data processed on behalf of the Controller according to agreement with the Controller.

Unless otherwise agreed in writing, costs for such measures shall be based on:

- Hourly rate for the time spent by the Processor, and
- the Level of complexity of the requested processing.

To the extent required by the legislation, the Processor may withhold Personal Data after termination of the Agreement which are subject to the technical and organisational security measures stated in this Data Processing Agreement.

11. Changes and additions

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

If any provision in this Data Processing Agreement becomes invalid this shall not affect the validity of the other provisions. The Parties shall replace the invalid provision with a valid provision which reflects the purpose of the invalid provision.

12. Liability

Liability for breach of the provisions in this Data Processing Agreement shall be regulated by the liability provisions in the Agreement concluded by the Parties. This also applies to any breaches by the Processor's sub-processors.

Both Parties are individually liable and shall be independently liable for the payment of all administrative fines and compensation directly to Data Subjects which may be imposed on the respective Party by authorities or courts pursuant to GDPR. Liability between the Parties shall be regulated by the Agreement.

Appendix A - Categories of Personal Data and Data Subjects

1. Categories of Data Subjects and Personal Data subject to processing under this Agreement

a. Categories of data subjects
   I. *Customer's employees*

b. Categories of personal data
   II. *Contact information such as name, address, email, telephone.*
   III. *Social Security No.*
   IV. *Job category;*
   V. *Employee number;*

c. Processing activities
   - *The Data Processor shall use IT systems to manage the Data Controller's time recording, transport expenses, additional records, images and documentation and the recording of goods. This data is exported into and is processed by Visma Løn.*
   - *In addition, the Processor is responsible for operation, testing, maintenance, development and fault correction of systems and applications. In order to optimise this, the Data Processor shall draw on the behaviour of individual user names in the application.*

2. Types of sensitive personal data subject to processing under the Agreement

The Controller shall notify the Processor of, and state below, any types of sensitive personal data in accordance with the current legislation on procession of personal data.

The Processor shall process information about the following on behalf of the Controller:	Yes	No
Racial or ethnic background or political, philosophical or religious belief		x
That a person is suspected of, charged with or convicted of a criminal offence		x
Health information		x
Sexual orientation		x
Trade union membership		x
Genetic or biometric data		x

Appendix B - List of current sub-processors

At the signing of this Agreement, the Processor's current sub-processors who may obtain access to the Controller's Personal Data include:

Name	Location/Country	Legal transfer mechanism if the sub-processor has access to personal data from countries outside the EU	Assisting the Processor with
Intempus ApS Staunings Plads 3 1607 København V CVR-no. 34696977	Denmark	Not applicable	Main supplier
DigitalOcean VAT ID: EU528002224	Germany	Not applicable	Data storage
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen VAT ID: DE812871812	Germany	Not applicable	Back-up data storage
Google Ireland Limited 3rd Floor, GOrdon House, Barrow street, Dublin 4 VAT ID: IE6388047V	Ireland	Not applicable	Data storage of attached documents (expenses, job descriptions, documentation of work performed, etc.)
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855, Luxembourg Registration No: B 186284	Germany	Not applicable	Data storage