Data Processing Agreement

VISMA

CONTENTS

1. Introduction

In connection with the Agreement between the Parties, the following Data processing agreement shall be applicable as of the date of signature between the Data Processor, Visma Enterprise and the Controller, the Customer, unless otherwise is explicitly stated in other agreements between the Parties.

The purpose of the Data processing agreement is to regulate how and for what purpose Visma Enterprise may process Personal data on behalf of the Customer, and to ensure that the Customer's Personal data is processed in accordance with guidelines and instructions as well as applicable law on data protection.

This Data processing agreement takes precedence over any conflicting provisions regarding processing of Personal Data in other agreements made between the Parties.

Categories of Personal Data, Data Subjects and processing of Personal data are outlined in appendix A.

2. 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).

3. The Controllers obligations

The Controller is responsible for the processing of Personal Data to meet the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act.

If using the services provided by the Data Processor under the Agreement, the Controller is obliged to process Personal Data in accordance with the provisions of applicable law on the processing of Personal Data.

The Controller is responsible for, inter alia, the existence of a legal basis for the processing performed by the Data Processor on behalf of the data controller.

4. The Processors obligations

The Processor shall only process Personal Data on behalf of and in accordance with the Controller's instruction.

Processing of Personal Data in the following manner:

only in accordance with applicable law,

to fulfil all obligations according to the Agreement,

as further specified via the Controller's ordinary use of the Processor's services and

as specified in this Data processing agreement.

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.

The Processor shall ensure the confidentiality, integrity and availability of Personal Data according to privacy legislation applicable to the Processor.

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.

The Data Processor ensures that the persons authorized to process Personal Data on behalf of the Data Controller have committed to confidentiality or are subject to appropriate statutory confidentiality.

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

The Processor will, by notifying the Controller without undue delay, and if possible within 24 hours, enable the Controller to comply with the legal requirements regarding notification to data authorities or Data Subjects about incidents.

Further, the Processor will to the extent it is possible and lawful notify the Controller of:

- requests for the disclosure of Personal Data received from a Data Subject,
- requests for the disclosure of Personal Data by governmental authorities, such as the police.

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 about this Agreement to governmental authorities such as the police, including Personal Data, except as obligated by law. The Processor does not have ownership, nor control with when and how the Data Controller uses third party integrations via the Data Processors API. The Data Controller is fully responsible and reliable for third part integrations.

5. Security

The Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, considering the technology and cost of implementation in relation to the risk represented by the Processing, and the nature of the Personal Data to be protected.

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

Further, the internal privacy framework developed by the Visma group aims to safeguard the confidentiality, integrity, security and availability of Personal Data. The following measures are of particular importance in this regard:

- Classification of Personal Data to ensure implementation of security measures equivalent to risk assessments.

- Assess use of encryption and anonymization as risk mitigating factors.

- Limiting access to Personal Data to those that need access to fulfil obligations according to this Agreement or the Service Agreement.

- Manage systems that detects, restore, prevents and reports privacy incidents.

- Security procedures as specified in appendix 6.1 Information Security, available at Visma Community.

If the Controller requires information about 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 a Processor, and imposes additional work on the Processor, the Processor may charge the Controller for such additional services.

The Processor notifies the Controller without undue delay after becoming aware of a breach of the personal data security of the Processor or any sub-processors.

6. Audit

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 (4) 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 multi-tenant 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.

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.

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.

The Controller shall be responsible for any costs arising from the Controller´s requested audits.

The Processor also invoices the Controller for assistance that exceeds the standard service that the Processor or the Visma Group makes available for compliance with applicable legislation on the processing of personal data.

7. Use of subcontractors and transfer of data

As part of the delivery of services to the Controller according to the Agreement and this Data Processor Agreement, the Processor may make use of subcontractors. Such subcontractors can be other companies within the Visma group or external third-party subcontractors.

The Processor shall ensure that subcontractors agrees to undertake responsibilities corresponding to the obligations set out in this Data processing agreement. All use of subcontractors is subject to the Visma group Privacy Statement.

The Controller may request to include an overview of the current subcontractors with access to Personal Data in an Appendix B. The Controller may also request a complete overview and more detailed information about the subcontractors involved in the agreements at any time.

The Controller shall be notified in advance of any changes of subcontractors that Process Personal Data. The Controller may object to changes if the Controller has reasonable, specific and practical reasons.

The Processor may not allow processing of Personal Data outside the EU/EEA without the consent of the Controller. .

If the Controller in the instructions in Appendix B or otherwise has given permission to a transfer of Personal data to a third country or to international organizations, the Processor must ensure that there is a legal foundation for the transfer.

8. Term and termination

This Data processing agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller according to the Service Agreements.

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.

Unless otherwise agreed in writing, the cost of such actions shall be based on:

- hourly rates for the time spent by the Processor and
- the complexity of the requested process.

The Processor may retain Personal Data after termination of the Agreement, to the extent it is required by law, subject to the same type of technical and organizational security measures as outlined in this Agreement.

9. Changes and amendments

Changes to the Data processing agreement shall be included in a supplement to to the Agreement and signed by both Parties in order to be valid.

If any provisions in this Data processing 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.

10. Liability

The liability for violation of provisions of this Data processing agreement shall be regulated by the liability clauses in the Service Agreements between the Parties. This also applies to any violation committed by the Processor's subcontractors.

Both parties are individually responsible and are shall be held independently liable to pay all administrative fees and indemnifications, which they are imposed by the authorities or courts in regards to the GDPR, directly to the Registered.

Appendix A - Categories of Personal Data and Data Subjects

1. Categories of Data Subject's and Personal Data subject to Processing according to this Agreement

   a. Categories of Data Subjects
      i. Customer end-users
      ii. Customer employees
      iii. Customer contact persons

   b. Categories of Personal Data
      i. Contact information such as name, phone, address, e-mail etc.
      ii. CPR number
      iii. Job category, information about salary, working hours, absence, pension, tax, bank account
      iv. other personal information necessary for the Controller to manage the employment relationship.

   c. Processing
      The Processor carries out the handling of the Controllers payroll administration, the preparation of payrolls, processing and storage of personal data of the Controller and Controllers employees, reporting and transfer of information to financial institution, banks, pension companies, mandatory reports in employers' associations, public boards (tax, statistics, etc.).
      In addition, the Data Processor is conducting test, maintenance, development and debugging in systems and applications.

2. Types of sensitive Personal Data subject to Processing according to the Agreement

The Controller is also responsible for informing the Processor of, and specifying below, any additional types of sensitive Personal Data according to applicable privacy legislation.

The Processor shall on behalf of the Controller, process information regarding:	Yes	No
Racial or ethnic origin, or political, philosophical or religious beliefs		x
That a person has been 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 - Overview current subcontractors

Current subcontractors of the Processor with access to the Controller's Personal Data upon signing this Agreement include:

Name	Location/country	Legal transfer mechanism if the subcontractor has access to personal data from countries outside the EU	Assisting the Processor with
Nets Denmark A/S Klausdalsbrovej 601 2750 Ballerup CVR no: 20016175	Denmark	Not applicable	Hosting Processing payroll
Atea A/S Lautrupvang 6 2750 Ballerup CVR no: 25511484	Denmark	Not applicable	Hosting Processing payroll
Puzzel A/S H.J. Holst Vej 5 2605 Brøndby CVR no: 25254864	Denmark	Not applicable	Phone system (replaces NetNordic November 10, 2021)
OnlineCity ApS Buchwaldsgade 50 5000 Odense C CVR no: 27364276	Denmark	Not applicable	Sending SMS regarding log-on
Cim Mobilty Fælledvej 17 7600 Struer CVR no: 27913334	Denmark	Not applicable	Sending mail and SMS regarding log-on
Visma IT & Communications AS Karenslyst Alle 56 0277 Oslo Org no: 979207379	Norway	Not applicable	Infrastructure Hosting file drives
Visma Labs SIA Sporta Street 11, Riga, LV 1013, Latvia Org no: 40103863798	Latvia	Not applicable	Development Debugging
PostNord Strålfors A/S Hedegaardsvej 88 2300 København S CVR no: 10068657	Denmark	Not applicable	Distribution of letters, change format and delivery to e-Boks
E-Boks Nordic A/S Hans Bekkevolds Allé 7 2900 Hellerup CVR no: 25674154	Denmark	Not applicable	Distribution of electronic messages (e-Boks)

Visma Software Labs AS, Karenslyst Alle 56 0277 Oslo Org no: 999256457	Norway	Not applicable	Development and reimbursement processing in connection with holiday card service and/or reimbursement
Visma Consulting A/S Gærtorvet 1 1799 København V CVR no: 29973334	Denmark	Not applicable	Software, support and development in connection with Mass upload e-Boks Electronic signature by Addo IT Service and infrastructure and network Nem.id/Mit.id for My Visma app (expected first half year 2022)
Itadel A/S Skanderborgvej 190 8260 Viby J CVR no: 37032034	Denmark	Not applicable	Hosting in connection with Mass upload e-Boks Electronic signature by Addo.
Visma Dataløn og ProLøn A/S Gærtorvet 3 1799 København V CVR no: 48117716	Denmark	Not applicable	Log-on module CRM
Netcompany A/S Grønningen 17, 1 1270 København K CVR no: 14814833	Denmark	Not applicable	Distribution of electronic messages (Mit.dk) (expected first half year 2022)