Data Processing Enclosure to Maventa™ Customer Agreement

Agreement

This enclosure is a intrinsic part of Maventa™ Customer Agreement and it regulates processing of personal data related to agreements paragraph 7. Personal Data.

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) from May 25th on.

The customer acts as the Controller for the data he has entered to Maventa service. The Processor operates in accordance with the Visma group Privacy Statement, available at https://www.visma.com/privacy-statement/, which is applicable to all companies within the Visma group.

In the Visma group Trust Center the Controller may find more information on how the Processor processes personal data. The purpose of this information is to enable the Controller to fulfill its duties to safeguard privacy when using a company within the Visma group to process personal data on their behalf. The Trust Center is available at https://www.visma.com/trust-centre/.

Scope of this enclosure

The Enclosure 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 of the Parties is not to transfer any Controller's statutory obligations to the Processor.

The purpose behind the Processor's Processing of Personal Data on behalf of the Controller is to fulfill the Customer Agreements and this Enclosure.

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

The Processor's obligations

The Processor shall only Process Personal Data on behalf of and in accordance with the Controller's instructions. By entering into this Enclosure, 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 Customer Agreement,

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

iv) as specified in this Enclosure.

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.

The categories of Data Subject's and Personal Data subject to Processing according to this Enclosure are outlined in Appendix A.

The Processor shall ensure the confidentiality, integrity and availability of Personal Data according to privacy legislation applicable to the Processor. The Processor has implemented systematic, organisational and technical measures to ensure a sufficient 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.

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, hereunder with regards to requests from Data Subjects and general privacy compliance according to GDPR article 32 to 36.

If the Controller requires information about security measures, documentation or information on how the Processor processes Personal Data in general, and such requests include information which exceeds what is necessary to comply with privacy legislation applicable to the Processor, then the Processor may charge the Controller for such additional services.

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

The Processor will, by notifying the Controller, 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 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

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 Enclosure to governmental authorities such as the police, hereunder Personal Data, except as obligated by law, such as through a court order or similar warrant.

The Processor does not manage or is not responsible how the Controller uses the API integration provided by the Processor or a similar third-party software which integrates the service provided by the Processor. The Controller is fully responsible for these integrations.

The Controller's obligations

The Controller confirms by the signing of this Enclosure that:

- This Enclosure fulfils the requirements of the Controller to have in place a written data processor agreement according to privacy legislation applicable in the Controller's country of establishment.
- The Controller shall, when using the services provided by the Processor under the Customer 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 Customer Agreement, not communicate any Sensitive Personal Data to the Processor, unless this is explicitly agreed in Appendix A to this Enclosure.
- 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.

Use of subcontractors and transfer of data

As part of the delivery of services to the Controller according to the Customer Agreements and this Enclosure, the Processor makes use subcontractors. Such subcontractors can be other companies within the Visma group or external third party subcontractors located within or outside the EU. The Processor shall ensure that subcontractors agrees to undertake responsibilities corresponding to the obligations set out in this Enclosure. 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. In addition, the Controller may find more information on subcontractors in the Visma Trust Center. The Controller may also request a complete overview and more detailed information about the subcontractors involved in the the Customer Agreements at any time.

If the subcontractors are located outside the EU, the Controller gives the Processor authorisation to ensure proper legal grounds for the transfer of Personal Data out of the EU on behalf of the Controller, hereunder by entering into EU Model Clauses or transferring Personal Data in accordance with the Privacy Shield.

If the Processor plans to change its use of subcontractors, the Controller shall be notified in advance. The Controller's right to object to such changes is limited to claiming that a new subcontractor, that process Personal Data on behalf of the Controller, is not compliant with applicable privacy legislation. After which the Processor shall demonstrate such compliance by giving the Controller access to the Processor's assessment of the new subcontractor in this regard. Upon further conflict, this shall be governed by clauses on remedies for breach of contract included in the Customer Agreement.

By signing this Enclosure, the Controller accepts the Processor's use of subcontractors as described above.

Security

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.

The parties agree in Customer Agreement separately the measures or other security procedures carried out by Processor in processing the Personal Data. The Controller is responsible for the appropriate and sufficient information security of the necessary equipment and IT environment.

Audit rights

The Controller may audit the Processor's compliance with this Enclosure 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.

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. Assistance from the Processor that exceed the standard service provided by the Processor and/or Visma group to comply with applicable privacy legislation, will be subject to fees.

Term and termination

This Enclosure is valid for as long as the Processor processes Personal Data on behalf of the Controller according to the Customer Agreements.

This Enclosure is automatically terminated upon termination of the Customer Agreement. Upon termination of this Enclosure, the Processor will delete if requested by Controller, or return in an appropriate format, Personal Data processed on behalf of the Controller under this Enclosure. The cost of such actions shall be agreed upon by the Parties and shall be based on; i) hourly rates for the time spent by the Controller, ii) the complexity of the requested process and iii) the requested format.

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

Changes and amendments

Amendments to the Enclosure may be done in accordance with Maventa™ Customer Agreements section 3. Modifications to this Agreement.

If any provisions in this Enclosure 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

For the avoidance of doubt the Parties agree and acknowledge that each Party shall be liable for and held accountable to pay any and all administrative fines which a Party has been imposed to pay in accordance with GDPR. The liability for any and all other violations of the provisions of this Agreement or obligations under GDPR shall be governed by the liability clauses in the Customer Agreements between the Parties. This also applies to any violation committed by the Processor's subcontractors..

Governing law and legal venue

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

****

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
        iv. Customer's customer data

    b. Categories of Personal Data
        i. contact information
        ii. user logs and IP addresses
        iii. bank account information

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

This section is only relevant if the Processor shall process sensitive Personal Data as indicated below on behalf of the Controller as part of the Services Agreement. In order for the Processor to process such data on behalf of the Controller, the types of Sensitive Personal Data in question must be specified below by the Controller.

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

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 with access to the Controller's Personal Data upon signing this Agreement.

Name	**Location/country**	**Legal grounds if the subcontractor has access to personal data from countries outside the EU**	**Assisting the Processor with**
Amazon Web Services Inc.	Luxembourg, Data center located in Germany	Not applicable within EU	Data center infrastructure and services
Danske Bank Oyj	Finland	Not applicable within EU	e-invoice delivery to Finnish bank network
Go2UBL	Netherlands	Not applicable within EU	Scanning services for Dutch and Danish customers
Kollektor A/S	Norway	Not applicable within EEA	Scanning services for Norwegian customers
Kollektor Oy	Finland	Not applicable within EU	Scanning services for Finnish customers
Nets A/S	Norway	Not applicable within EEA	e-invoice delivery to Norwegian bank network and printing services
Postnord Strålfors Oy	Finland	Not applicable within EU	Printing services
SendGrid Inc	United States of America	Privacy Shield certified, Data protection agreement including EU standard clauses	Email invoices