

SERVICE CONDITIONS FOR VISMA SIGN SERVICES AND PERSONAL DATA PROCESSING

The essential features of Visma Sign services, the commitments of Visma Solutions Oy to the Service users, and the principles concerning the processing of personal data have been outlined in this summary.

The Service conditions are provided in full directly below this summary. Terms and information concerning personal data processing are included in both the terms of service and data processing enclosure below and privacy policy of Visma Solutions Oy which can be read at https://vismasign.fi/download/visma_sign-privacy_policy.pdf

The Service can be used for electronically signing agreements between yourself and your contracting partners, for sending agreements to your contracting partners for signing, for receiving signing requests from your contracting partners, and for saving and filing agreements you have signed in the electronic archive of the Service.

In the Service, all Service users are always identified using the strong electronic identification method stipulated in the law. This way you can be certain of the reliability of the signatures provided in the Service.

All personal data submitted to the Service shall always be processed and stored in accordance with the applicable personal data legislation.

The rights to the material saved in the Service shall not be transferred to the service provider.

You have the right to terminate the Service with a one (1) month notice period.

GENERAL SERVICE CONDITIONS FOR THE USE OF VISMA SIGN SERVICES

1. APPLICATION AND ENTRY INTO FORCE OF THE SERVICE CONDITIONS

These service conditions ('Service Conditions') of Visma Solutions Oy ('Supplier') shall be applied to the below-specified Services they provide for their customers ('Customer') for the part that has not been otherwise agreed between the parties in writing. The implementation of the Services requires the acceptance of these Service Conditions. These Service Conditions enter into force on 01.01.2018 and shall remain in force until further notice.

The agreement between the Supplier and Customer on Service provision shall enter into force as binding for the Supplier and Customer when (i) the Customer has accepted the offer concerning the Services, (ii) the parties have separately signed the agreement

concerning the Services on paper, (iii) the parties have otherwise agreed upon Service provision using electronic identification, or (iv) the Customer has implemented the Service.

The Supplier's offer, the confirmation concerning Service provision, or the agreement between the parties with its appendices form the entire agreement between the parties replacing the possible previous discussions and correspondence concerning the Services. If there are discrepancies between the agreement documents and these Service Conditions, the application of these Service Conditions shall take primacy. If there are discrepancies between the appendices to the agreements between the parties, the appendices shall be applied in numerical order.

Under these Service Conditions, the Customer can, at their own initiative, download agreements and send notifications concerning agreements to be signed by the other Contracting Party, receive signing requests, sign agreements using Electronic Signature, and save the signed agreements in the Electronic Archive.

Information provided in the Service shall be stored and processed in accordance with the applicable personal data protection legislation and these Service Conditions.

THESE SERVICE CONDITIONS DO NOT IN ANY WAY RESTRICT THE RIGHTS OF CONSUMER CUSTOMERS UNDER THE CONSUMER PROTECTION LEGISLATION.

2. DEFINITIONS

'Customer' refers to the entity using the Service who has agreed to use the Service in accordance with these Service Conditions and other agreement documents. The Customer shall be responsible for providing the Service users with the company's signatory right.

'Customer's material' refers to information or material transferred to the Service by the Customer or to information or material supplied or made available to the Supplier on behalf of the Customer for the Service and to other information or material defined as the Customer's material by the parties.

'Electronic Archive' refers to the part of the Service where the Customer may save their own signed agreements.

'Electronic Signature' refers to agreement signing with the aid of the TUPAS solution designated by Finnish banks, mobile identification mechanisms or other electronic identification methods approved by legislation, or a separate signature mechanism determined by the Supplier and provided by a third party. Electronic identification shall always take place i) using an electronic identification method that meets the high security level criteria referred to in Article 8, paragraph 2, subparagraph b in the EU Regulation No 910/2014 on electronic identification and trust services or the high

security level referred to in subparagraph b in the said paragraph, and ii) using a strong electronic identification method which is in accordance with the Finnish Act (7 August 2009/617 with subsequent amendments) on Strong Electronic Identification and Electronic Signatures, or iii) using a strong electronic identification method which is in accordance with other applicable legislation concerning electronic identification in effect in the country where the customer is located.

'Electronic Agreement' refers to an agreement that has been signed using Electronic Signature.

'Service' refers to the Internet-based service provided by the Supplier, with the aid of which Agreement Requests can be sent and/or received and electronically signed and with which verified Electronic Agreements can be saved in the Electronic Archive.

'Privacy policy' refers to the Supplier's up-to-date privacy policy concerning personal data processing and storing which can be read at https://vismasign.fi/download/visma_sign-privacy_policy.pdf

'Agreement Request' refers to an electronic message that the Customer sends to the Contracting Party as an indication of a request to sign the agreement.

'Contracting Party' refers to the Customer's own customer or other contracting party, to whom the Customer sends or from whom the Customer receives an Agreement Request to electronically sign an agreement.

3. SERVICE USE

3.1. GENERAL CONDITIONS

The Supplier has the right to amend the Service, its availability and the requirements set for the hardware necessary for its use in a way that does not change the key functionalities of the Service. The Service may include services or other content, which are offered as part of the Service, provided by third parties and specified in the service descriptions. The Supplier's liability for the faults in and the availability of services and content provided by third parties is limited to the rights the Supplier has in relation to the third party.

The Supplier shall announce possible significant changes concerning the Service a reasonable period of time in advance. The announcement shall be made at the Service website. Technical changes, such as hardware or software updates, shall not be separately announced.

The Supplier has the right to suspend Service provision if it is necessary due to the Service, the technical changes in or upgrading of the Service, the installation, modification or maintenance work carried out on the general communications network, or if the laws or regulations or the provisions, instructions or recommendations of the authorities applicable to the Service so

require. The Supplier shall work towards preventing the service interruption from lasting for an unnecessarily long period of time and keeping the resulting disadvantages to a minimum. If possible, the Supplier shall announce the service interruptions a reasonable period of time in advance. The announcement shall be made at the Service website. The service may use cookies, the purpose of which is to provide the Customer with faster Service use. The Customer may disable cookies by changing their browser settings. Disabling cookies may decrease the usability of the Service.

The Supplier has the right to prevent the Customer from accessing the Service if the Supplier suspects the Customer of misusing the Service or burdening the Service in an exceptional way. The Supplier must inform the Customer without unnecessary delay of the reasons for preventing them from accessing the Service, except in situations where the Supplier or the authorities have reason to suspect that the Service is being used for illegal activities. The Customer agrees to use the Service in accordance with the Service Conditions, the law, and good practice. The Service shall not be used in a way that is disadvantageous, offensive or damaging to the Supplier, the Supplier's cooperation partners, another user, or a third party. Operations which are against the Service Conditions include, i.a., activities connected with money laundering, trafficking narcotics or other illegal substances, or betting.

The Supplier has the right to amend these Service Conditions by announcing the matter at the Service website at least two (2) months before the new Service Conditions enter in to force. The new Service Conditions shall enter into force as binding for the Customer on their inception date, unless the Customer has terminated, in accordance with section 7, the agreement so that it ends before the inception date.

3.2. SERVICE PURCHASE

The Customer shall purchase the Service by providing the information required by the Service and making the payment presented in the Service or other payment agreed between the parties.

3.3. ATTACHMENT OF ELECTRONIC AGREEMENT MATERIAL

The Customer shall transfer the agreement to be signed from their own terminal device to the Service. The transferred material is displayed as a separate file in the SSL-protected Service.

3.4. SENDING AN ELECTRONIC AGREEMENT REQUEST

The Customer shall enter the contact information of the Contracting Parties and other required identification details into the Service. The system creates a temporary disposable password, with which the Contracting Party can log into the Service. Before logging into the Service and signing the agreement, the Contracting Party must, for their part, accept the Service's conditions of use. When the agreement has been signed, the

temporary password will expire. The Customer shall ensure that the information concerning the Contracting Party is correct.

3.5. ELECTRONIC SIGNATURE

The Customer and the Contracting Parties shall sign the agreement in the Service by Electronic Signature.

3.6. USING THE ELECTRONIC ARCHIVE

The Customer may save, browse and specify separate files in the Electronic Archive. The Customer is responsible for the archive use, rights and access rights of users. The right to save in the archive shall remain in force for the time being. The archive content can be separately retrieved and saved for 30 days after the Service has been ended by the Customer.

3.7. SEARCHING FOR THE CUSTOMER'S AGREEMENTS

Unless separately otherwise agreed, the Service does not include searching for or retrieving the Customer's Electronic Agreements in the Supplier's systems. If the Supplier searches for and retrieves Electronic Agreements in their systems at the Customer's request, the Supplier has the right to charge a fee in accordance with their current price list.

3.8. PAYMENTS

The prices charged for the Service and the terms of payment regarding them have been specified in the Supplier's offer or the agreement between the parties. Unless a price for the Service has been separately agreed upon, the prices in the Supplier's current price list shall be applied. Unless the terms of payment have been agreed upon, the term of payment is 14 days net from the date on the invoice. Penalty interest is set according to the Interest Act. Value added tax is added to the prices in accordance with the provisions currently in force.

The Supplier has the right to amend the price of the Service by announcing the matter on the Service website at least two (2) months before the amended prices enter into force. The period of two months begins at the end of the calendar month during which the announcement and the amended prices have been published on the website. The announcement shall have no effect on the prices of the Services delivered, or paid for in advance by the Customer, before the amendment enters into force. If the Customer objects to the entry into force of the amended prices as a whole or in part, the Customer shall inform the Supplier of this at least 30 days before the amended prices enter into force. If the Customer objects to the entry into force of the amended prices and if the parties do not otherwise agree, the agreement between the parties shall end on the entry into force date of the amended prices for the parts of the Service whose price change the Customer has opposed.

If the Customer's payment has been delayed for over 14 days from the due date, the Supplier has the right to prevent the Customer from accessing the Service until the Customer has paid all overdue payments to the Supplier and/or terminate the agreement in accordance with section 7.

4. SERVICE CONTENT AND IMMATERIAL RIGHTS

All the rights related to the Service and its content, excluding the copyrights, trademark rights and other immaterial rights connected with the Customer's Material, belong to the Supplier or third parties. The Customer has the right to use the Service only in accordance with these Service Conditions. The Customer does not have the right to, without the Supplier's consent, copy, save, transfer, distribute or in any other way make the Service, its parts or any other material contained by the Service, available to the public in any other way than the ones specifically stated in these Service Conditions. The Customer has the right, within the limits of the provided access rights, to freely browse and use the Service and the contained material in their own business operations during the validity period of the access right. The copyrights, trademark rights and other immaterial rights related to the Customer's Material shall belong to the Customer or a third party. The Customer declares that they have the right to save all the Customer's Material in the Service.

5. PERSONAL DATA PROCESSING

Parties agree to be comply in their own operations with the data protection regulation applicable to them, such as the EU's general data protection regulation.

The Supplier may also process personal data on Customer's behalf. In this case the terms and conditions of the processing are defined solely in attached data processing enclosure.

In addition to the above mentioned, the Supplier shall process, as the data collector, the personal data provided by the Customer in connection with Service registration for invoicing, marketing and customer service purposes. Supplier may also process the information given or updated by Customer. Further details of this processing is described in attached data processing enclosure.

Both parties shall be responsible for ensuring, for their own part, that the equipment and data communications as well as other technical and physical environment have been protected against data security risks in accordance with the relevant data security practices and that the procedures regarding protection and data backup are followed.

6. FORCE MAJEURE

Neither party shall be liable for delay or damage that is caused due to an obstacle beyond the party's or their subcontractors' control that the party cannot reasonably be required to have considered at the moment of concluding the agreement and the consequences of which the party could not reasonably have avoided. A strike, lock-out, boycott, or other industrial action is also considered a force majeure situation when the party itself is a target of or is involved in such actions. A party must inform the other party of the force majeure and its cessation without delay.

7. TERMINATION AND VALIDITY OF THE AGREEMENT

Both parties shall have the right to terminate the agreement with a one (1) month notice period by informing the other party of this in writing. The notice period begins at the end of the calendar month during which the notice of termination has been submitted. A party shall have the right to terminate the agreement concerning the Service with immediate effect if the other party (i) is in material breach of the terms of agreement and has not repaired the breach of agreement within 14 days of receiving a written repair request from the other party, (ii) is declared bankrupt or put into liquidation, or has otherwise ceased payment. If a party terminates the agreement in accordance with this section 7, the Supplier shall have the right to charge the Customer for all the fees, costs and payments incurred before the expiry of the agreement.

Unless otherwise agreed in writing, the Supplier shall deliver the Customer's Material to the Customer within 14 days of the expiry of the Service's access rights or at the Customer's written request. The Customer's Material shall be delivered in the same generally used electronic form in which it has been filed in the Service. The Supplier has the right to charge the Customer for collecting, processing, and releasing data in accordance with the stipulated charging principles. After this, the Supplier shall destroy the Customer's Material without unnecessary delay. The Supplier does, however, have the right to save the Customer's Material for the part that the Supplier is obligated to do so on the basis of the law or official regulations.

8. LIABILITIES AND LIMITATIONS OF LIABILITY

The Supplier shall do their best in order for the Service to beat the Customer's use 24/7 in accordance with the service description. The Supplier agrees to repair the faults occurring in the Service or its availability without unnecessary delay. The Supplier's liability for the faults in the Service is limited to the obligation to repair agreed upon above.

The Supplier is not liable for the functionality of the hardware or software used by the Customer or their compatibility with the Service. The Customer shall be responsible for the procurement of the devices, connections and software needed for the use of the Service and for keeping them operational. The Customer shall be responsible for the protection of their own operating

environment and the costs related to Service use, such as data communications costs. The Customer is aware that the Internet as an operating environment may cause data security risks and defects in the Service functionality.

The Supplier shall not be liable for the operation of third-party identification services or other services or their non-functioning or the possible damages they have caused to the Customer.

The Supplier shall not be liable for agreements or other documents, or their content, saved in the Service. The Customer is responsible for ensuring that the Customer's Material does not contain harmful software or other data security risks. The Customer is responsible for taking care of the backup copying of the Customer's Material. The Service may contain links to websites owned or managed by third parties. The Supplier is not responsible for the content of such websites or the services or products offered on them.

The Supplier's overall liability in connection with the Service is no more than the total sum of the payments made by the Customer for the Service during the past 12 months or, if the Customer has not paid for the Service, one thousand (1,000) euros.

9. IDENTIFICATION SERVICES

The Service uses i) electronic identification services provided by third parties that meet the high security level criteria referred to in Article 8, paragraph 2, subparagraph b in the EU Regulation No 910/2014 on electronic identification and trust services or the high security level referred to in subparagraph b in the said paragraph and ii) strong electronic identification services provided by third parties which are in accordance with the Finnish Act (7 August 2009/617 with subsequent amendments) on Strong Electronic Identification and Electronic Signatures, or iii) strong electronic identification services provided by third parties which are in accordance with other applicable legislation concerning electronic identification in effect in the country where the customer is located. The Supplier shall be responsible for compliance with and careful application of conditions concerning third-party identification services. The Supplier shall not be otherwise responsible for the identification services or possible technical or operational faults occurring therein.

10. OTHER TERMS

One party shall not have the right to transfer the agreement between the parties without the written consent of the other party. One party shall, however, have the right to transfer the agreements between the parties to their group entities or, in connection with the transfer or reorganisation of business operations, by informing the other party of this in writing. The party that has transferred the agreements is responsible for informing the other party of the matter.

Finnish law shall be applied in the Agreement and Service, excluding its provisions on the choice of law. Any disputes concerning the Agreement and Service shall be settled finally in arbitration proceedings in accordance with the arbitration proceeding rules issued by the Finnish Central Chamber of Commerce. The Court of Arbitration has one member. The location of the arbitration proceedings is Helsinki, Finland, and the language of the arbitration proceedings is Finnish.

A Consumer Customer has the right to submit the dispute concerning the Service and the related agreement to be settled by the Finnish Consumer Disputes Board or other equivalent body.

Data Processing Enclosure for Visma Sign Service Conditions

Agreement

This enclosure is a intrinsic part of Visma Sign service conditions and it regulates processing of personal data related to agreements paragraph 5. 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 Visma Sign 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 Visma Sign service conditions section 7. Termination and validity of the 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 employees
 - ii. private persons

- b. Categories of Personal Data
 - i. full name of the person

- ii. address
- iii. contact information
- iv. user logs and IP addresses
- v. the name of the bank or operator who makes the identification
- vi. personal identification number
- vii. sequential number replacing ID code after the ID has been removed after identification
- viii. business code

Appendix B - Overview current subcontractors

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

In the future, an up-to-date list can be found at the address:

<https://privacy.vismasolutions.com>:

Name	Location/ country	Legal grounds if the subcontractor has access to personal data from countries outside the EU	Assisting the Processor with
Fraktio Oy	Finland	Not applicable within EU	Technical development and maintenance of the service
Druid Oy	Finland	Not applicable within EU	Technical development of service parts
Upcloud Oy	Finland	Not applicable within EU	Data center services