

## 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. Visma Trust Centre provides details about how Visma processes personal data in our software: <https://www.visma.com/trust-centre/privacy/>

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://vismasolutions.com/tietosuojat/> (in Finnish). The Supplier processes personal data in accordance with the Visma Group's privacy policy: <https://www.visma.com/trust-centre/>

**'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 into 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 are described in attached data processing enclosure and in Visma Group's privacy policy: <https://www.visma.com/trust-centre/privacy/>

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.

## Appendix: Data Processing Agreement

This Appendix is an integral part of the Service Conditions for Visma Sign and Personal Data Processing in connection with the Visma Sign service. Obligations regarding Personal Data processing are agreed in the Section 5 of the Service Conditions.

### 1. Definitions

The definition of Personal Data, Special Categories of Personal Data (e.g., Sensitive Personal Data), Processing of Personal Data, Data Subject, a Controller and a Processor is equivalent to how the terms are used and interpreted in applicable data privacy legislation, including the General Data Protection Regulation (GDPR) applicable for this Agreement and Europe from 25 May 2018.

Service Conditions refer to the Service Conditions for Visma Sign or any other agreements between the parties ("**Service Conditions**") and this Appendix is an integral part of the Service Conditions and shall be signed by the parties ("**DPA**").

A customer acts as a Controller of the data in and Visma Sign service. Visma Solutions Oy acts as a Processor and complies with the privacy statement of Visma Group that is available at <https://www.visma.com/privacy-statement/international/> which is applied to all Visma Group companies.

### 2. The Scope

This DPA regulates the Processing of Personal Data by the Processor 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. However, this does not transfer any legal obligations of the Controller to the Processor.

In cases of conflict, this DPA has priority over any conflicting provisions regarding the Processing of Personal Data in the Service Conditions for Visma Sign or any other agreements between the parties. This DPA shall be valid until any service agreement containing Processing of Personal Data is valid between the parties.

#### **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 DPA, the Controller shall instruct the Processor to process Personal Data in the following manner:

- i. only in accordance with applicable law;
- ii. to comply with any obligations under the Service Conditions;
- iii. in the manner specifically determined by the Controller in connection with the normal use of the Processor's services and;
- iv. as specified in this DPA.

The Processor shall notify the Controller when receiving information about any instructions or other processing measures of the Controller which, in the Processor's opinion, violate the applicable data protection regulations.

The categories of Data Subjects and Personal Data subject to be processed in accordance with this DPA are listed in Section A below.

The Processor shall assist the Controller by appropriate technical and organisational measures, taking into account, where possible, the nature of the processing and the data available to the Controller, to fulfil the Controller's obligation to respond to requests by the Data subjects under Section 3 of the GDPR and to ensure privacy as required by Articles 32-36 of the GDPR.

If the Controller requests information or assistance on security measures, documentation or other information related to the Processor's processing of personal data, and the content of the requests deviates from the standard information or assistance provided by the Processor under the applicable data protection regulations and results in additional work for the Processor, the Processor may charge the Controller for additional services.

The Processor shall ensure that the persons entitled to Process Personal Data are bound by an obligation of professional secrecy or are subject to an appropriate legal obligation of professional secrecy.

The Processor shall, without undue delay, notify the Controller of data breaches so that the Controller can fulfil its statutory obligation to report data security breaches to the Data Protection Authorities and the Data Subjects.

In addition, the Processor shall notify the Controller of the following matters to the extent appropriate and lawful:

- i. Requests by the Data Subject for access to Personal Data,
- ii. requests for access to Personal Data by public authorities, such as the police

The Processor will not respond directly to the Data Subjects' requests unless the Controller has authorised the Processor to do so. The Processor shall not grant access to Personal Data processed under this DPA to authorities, such as the police, other than in accordance with the law, such as a court decision or other similar order.

The Processor does not manage and is not responsible for the way in which the Controller uses the API or similar to integrate a third-party software to the Processor's service. The Controller is fully responsible for these integrations.

## **The Controller's responsibilities**

When approving this DPA, the Controller shall confirm the following:

- i. This DPA meets the requirements of the Data Protection Law of the Controller's country of establishment regarding the Controller's written agreement on the Processing of Personal Data.

- ii. The Controller shall process Personal Data in accordance with the applicable data protection regulations when using the services provided by the Processor in accordance with the Service Conditions.
- iii. The Controller has a statutory right to process and transfer the Personal Data in question to the Processor (including subcontractors used by the Processor).
- iv. The Controller has legal authority to process and disclose to the Processor (including any subcontractors used by the Processor) the Personal Data in question.
- v. The Controller is solely responsible for the accuracy, integrity, content, reliability and legality of the Personal Data provided to the Processor.
- vi. The Controller has complied with all mandatory notifications to authorities regarding the Processing of Personal Data and with the obligations and requirements for obtaining authorisations.
- vii. The Controller has fulfilled his obligation to provide relevant information related to the Processing of the Data subjects' Personal Data in accordance with the mandatory data protection regulations applicable to the Data Subjects.
- viii. The Controller shall use the services provided by the Processor in accordance with the Service Conditions and shall not transmit Sensitive Personal Data to the Processor except in the cases explicitly specified in Section A of this DPA.
- ix. The Controller shall maintain an up-to-date register of the types and categories of Personal Data which it processes which differ from the types and categories of Personal Data referred to in Section A of this DPA.

### 3. Subcontractors and Transfer of Personal Data

The Processor has the right to transfer Personal Data for the purpose of carrying out the service within the European Union, the European Economic Area, or other countries identified by the European Commission as guaranteeing an adequate level of data protection. In order to implement the service, the Processor also has the right to transfer Personal Data outside the European Union or the European Economic Area, in accordance with the data protection legislation. At any time, the Controller has the right to receive information on the location of the processing of Personal Data from the Processor <https://privacy.vismasolutions.com>. If Personal Data is processed outside the European Union or the European Economic Area, each Party shall contribute to ensuring compliance with data protection law with regard to the Processing of Personal Data.

The Processor may use subcontractors to provide services to the Controller in accordance with the Service Conditions and this DPA. Such subcontractors may be other Visma Group companies or external subcontractors located inside or outside the EU. The Processor shall ensure that subcontractors undertake to comply with obligations equivalent to those set out in this DPA. The Visma Group's data protection guidelines apply to all use of subcontractors.

Section B of this DPA lists the current subcontractors of the Processor who have access to Personal Data. The Controller may also, at any time, request a full overview and more detailed information on the subcontractors involved in the Service Conditions. This review may be submitted to the Controller via a website dedicated to the data protection of the Processor.

The Processor has the right to change subcontractors during the term of the Service Conditions. The Processor shall notify the Controller in advance of any changes in the subcontractors processing Personal Data. The Controller shall have the right to object to such changes for a justified reason. The Controller shall notify the objection without undue delay after receiving information from the Processor. If the Controller does not accept the change or addition of a subcontractor, the Processor shall have the right to terminate the service agreement with 30 days' notice.

By accepting this DPA, the Controller agrees to the use of the Processor's subcontractors as described above.

## 4. Data Protection

The Processor is committed to providing high quality products and services with regards to safety. The Processor shall ensure appropriate security through organisational, technical and physical security measures equivalent to those under Article 32 of the GDPR, taking into account state-of-the-art technology and implementation costs in relation to the processing risks and the nature of the Personal Data to be protected.

The Parties shall, in the Service Condition, separately agree on the measures or other data security procedures that the Processor shall implement with regard to the Processing of Personal Data. The Controller shall be responsible for the appropriate and adequate security of the necessary equipment and the IT operating environment under his responsibility.

## 5. Inspection Rights

The Controller may audit the Processor's compliance with this DPA no more than once a year. The Controller may request more frequent audits if required by the legislation applicable to the Controller. When requesting an audit, the Controller shall submit to the Processor a detailed audit plan indicating the planned scope, duration and start date of the audit, at least four (4) weeks before the planned start date of the audit. If the audit is carried out by a third party, this must be agreed between the two parties. If the processing of data takes place in an environment used by the Processor's other clients or other third parties, the Processor may require that, for security reasons, the audit is performed by a neutral third party chosen by the Processor.

If the content of the requested audit has been addressed in an ISAE, ISO or similar report prepared by a third auditor during the previous 12 months, and the Processor confirms that no material changes have occurred in the audited activities, the Controller undertakes to accept the results of the report and does not require a re-audit for the activities included in the report.

In any case, the audits shall be carried out during normal business hours in the Processor's location in accordance with the Processor's own practices and shall not unduly interfere with the Processor's business operations.

The Controller shall be responsible for all costs of the audits it requests. The Processor has the right to charge the Controller for assistance provided in compliance with the applicable data protection regulations that exceeds the service provided by the Processor and/or the Visma Group to the Controller in accordance with the DPA or Service Conditions.

## 6. Duration and Termination

This DPA shall be valid as long as the Processor processes Personal Data on behalf of the Controller in accordance with the Service Conditions.

This DPA shall terminate automatically upon termination of the Service Conditions. Upon the expiration of this DPA, the Processor shall delete or return the Personal Data processed on behalf of the Controller in accordance with the terms of the Service Conditions. Unless otherwise agreed in writing, the costs of this shall be calculated based on:

- i. the hourly rate of the Processor and the number of hours spent on this work and
- ii. the complexity of the action required.

The Processor may retain personal data after the termination of the Service Conditions to the extent required by law and subject to the corresponding technical and organisational security measures set out in this DPA.

## 7. Changes and Additions

The terms of the Service Conditions of Visma Sign -service section 7. "Termination and Validity of the Agreement" shall be applied to the amendments of this DPA.

If any terms of this DPA are held to be invalid, this will not affect the validity of the other terms of this DPA. The parties shall replace the invalid term with a legal term, the purpose of which corresponds to the invalid term.

## 8. Liability

The parties have agreed the following:

If the Data Subject suffers damage as a result of a breach of the GDPR, each party shall be personally liable for the damage caused to the Data subject in accordance with Article 82 of the GDPR. Each party is also responsible for any administrative fines imposed on it by a supervisory authority under Article 83 of the GDPR.

In other respects, liability for breach of the Service Conditions or any other claim related to the GDPR is defined in Section 8 "Liabilities and Limitations of Liability" of Visma Sign Service Conditions. The condition also applies to violations by the Processor's subcontractors.

### A. Categories of Data Subjects and Types of Personal Data Processed

- a. Categories of Data Subjects

- i. the personnel of the Customer
  - ii. private individuals
- b. Types of Personal Data Processed
- i. full name of the person
  - ii. physical address
  - iii. contact information
  - iv. logs and IP addresses of the users
  - v. the name of the bank or operator issuing the identification
  - vi. social security number
  - vii. sequential number changed from the social security number when social security number has been deleted after the identification
  - viii. business ID

## B. Existing Subcontractors

The up-to-date information of the Visma subcontractors that are participating in the production of Visma Sign -service and thus are processing personal data saved in the Visma service by the controller after the acceptance of this DPA are listed in the table at <https://vismasolutions.com/tietosuoja/henkilotietojen-kasittely-visma-signissa>

Currently all sub-processing of personal data is occurring within the EU/ETA and no data is transferred outside the EU/ETA.