GENERAL TERMS AND CONDITIONS FOR VISMA ADDO

VERSION 3.1, MAY 2019

1 INTRODUCTION

1.1 These subscription terms and conditions are accepted by ticking the box "I have read and accept the subscription terms and conditions" on the order form, by using the Solution or otherwise expressing your acceptance hereof and apply to Visma Consulting A/S, Nørgaardsvej 32, 2800 Lyngby, business reg. no.: 29973334 ("Visma") and the customer (the "Customer"). If the Customer is a legal person, these General Terms and Conditions are accepted on behalf of the Customer.

1.2 The below General Terms and Conditions stipulate the Parties' rights and obligations in connection with the Customer's use of the digital signing solution, Visma Addo (the "Solution").

1.3 The Solution is developed for businesses and authorities (as opposed to consumers).

2 DEFINITIONER

2.1 The following definitions apply:

2.1.1 The "Agreement": The agreement between the Parties regarding the Customer's use of the Solution which is regarded as concluded upon the Customer's acceptance of the General Terms and Conditions.

2.1.2 The "Customer": The business or authority using the Solution.

2.1.3 The "Solution": Visma's digital signature solution. See a detailed description thereof on www.vismaaddo.dk.

2.1.4 The "Party"/"Parties:" The Customer and/or Visma according to the context.

2.1.5 The "General Terms and Conditions": The general terms and conditions for the Solution.

2.1.6 "Transaction": A Transaction is composed of one or several of the following steps:

- Notification: Notification to the receiver on the receipt of one or more documents to be signed.
- Identification: The option of requiring identification from the recipient before signing
- Signing: The recipient can sign documents with the signing options available in the Solution
- Distribution: The option to distribute the signed documents through the channels available in the Solution

1.1.1 "Credits": The "currency" the Customer acquires and can use as payment for Transactions in the Solution. Each Transaction costs a number of Credits depending on the costs Visma has in connection with the individual Transaction.

3 THE CUSTOMER'S USER RIGHT ETC.

3.1 Visma owns all rights to the Solution, including copyright, trademarks and other intellectual property rights.

3.2 Against payment of the agreed fee, the Customer receives a non-exclusive right to use the Solution in

accordance with these General Terms and Conditions.

3.2.1 The user right further applies for the Customer's affiliated companies.

3.2.2 The user right applies for an unlimited number of users at the Customer and the Customer's affiliated companies.

3.3 The Solution can be accessed and used by using a username and password forwarded by Visma to the Customer.

3.3.1 The Customer is responsible for storing the username and password securely and confidentially to ensure that the username and password is only used for the Customer's use of the Solution.

3.3.2 The Customer is responsible for the creation of users and the administration of user rights to the Solution.

4 EFFECTIVE DATE AND DURATION

4.1 The Customer can use the Solution after the Agreement has been concluded, i.e. after the Customer has created an account and has accepted these General Terms and Conditions.

4.2 When the Agreement has been concluded, the Customer will receive a username and password for the Customer's administrator of the Solution.

4.3 The Agreement can be terminated by Visma with a notice of 6 months to the end of a calendar month.

4.4 If the Agreement is terminated by Visma, the Customer is responsible for using all Credits during the termination period. Any unused Credits at the expiry of the Agreement will not be refunded or made available to the Customer.

5 OPERATION AND MAINTENANCE

5.1 Visma is obligated to ensure a stable and continuous operation of the system, including ongoing maintenance by correcting errors and inconveniences.

5.2 All planned maintenance will not, to the extent possible, be performed in the period from 08.00 – 18.00 on working days. In extraordinary circumstances, immediate remedy of errors or installation of changes for security or system critical reasons may be necessary. In such situations, Visma is entitled to close down all or part of the system outside the stated maintenance period.

5.3 Based on the Customer's inquiries and Visma's own monitoring of the Solution, Visma will perform error recovery of the Solution.

5.4 Visma further performs ongoing preventive maintenance of the Solution and the operating environment in order to ensure a stable operation and a high level of security. All preventive maintenance will not be performed within the period 08.00 – 18.00 on working days, cf. clause 5.2

6 CHANGES

6.1 Visma is entitled to make ongoing updates and improvements to the Solution. Visma is also entitled to change the composition and construction of the Solution and the services therein. These updates, improvements and changes may be implemented with or without notice and may affect the services, including any information and data uploaded to or produced by the Solution.

6.2 Notices in accordance with clause 6.1 will be displayed on Visma's website under "Support".

7 SUPPORT

7.1 The Customer can request support of the Solution during the period 8.30-17.00 CET on Visma's website

under "Support".

8 FEES AND PAYMENT

8.1 The Customer can buy Credits on an ongoing basis. The fee for additional Credits, volume discounts and prices of the individual transaction types are indicated on www.vismaaddo.dk.

8.2 The Customer may choose to select "automatic top-up" of the account. This way, the Customer automatically receives a prior agreed number of Credits transferred to the account, when all Credits on the account have been used. When using automatic top-up, the fee for the Credits is automatically withdrawn from the credit card registered with the Customer's account.

8.3 If the Customer has not used the Solution for a period of 24 consecutive months, any unused Credits will expire.

8.4 Fees for purchased Credits cannot be refunded in any circumstances, including when the Agreement expires.

9 PERSONAL DATA AND SECURITY

9.1 The Customer is the data controller as regards to the personal data uploaded by the Customer and processed by the Customer in the Solution, whereas Visma is the data processor of such data. The Agreement includes a data processing agreement enclosed as appendix 1 (hereinafter the "Data Processing Agreement"), to which reference is made with regard to further information on Visma's processing of the Customer's personal data.

9.2 The Customer's data is processed and stored securely and Visma warrants that the Solution at all times is technically configured in accordance with current good IT security practices and that the appropriate technical and organizational security measures have been implemented.

9.3 Visma is entitled to process the Customer's transaction and subscription data and user patterns in an anonymized form during and after the expiry of the Agreement for statistics and analysis purposes and to improve the Solution.

10 CONFIDENTIALITY

10.1 Visma must observe an unconditional duty of confidentiality as regards to information on the Customer and the Customer's customer to which Visma gains access when the Customer uses the Solution, with the exception of information which is already disclosed to the public. Visma may not give a third party access to the information or use the information for other purposes than to fulfil the Agreement. Further, Visma must ensure that the Customers using the Solution do not gain access to each other's' information.

10.2 The duty of confidentiality remains in force after the expiry of the Agreement.

10.3 Visma is entitled to use the Customer's name for marketing purposes, including as a reference.

10.4 The Customer must keep all usernames and passwords confidential. If the Customer loses a username and/or password or if there is a risk that these have been disclosed to an unauthorized person or otherwise have been compromised, the Customer must inform Visma hereof.

11 RENTENTION OF DATA AND BACK-UP

11.1 When a transaction has been completed, the signed document will be stored for 10 days after which it is automatically deleted. Data regarding the transaction will not be deleted.

11.2 Visma performs a daily backup of the Solution and the Customer's data. The back-up is stored for 30

days. Visma is responsible for ensuring that backup copies are stored securely.

12 LEGAL AND REGULATORY REQUIREMENTS

12.1 Each Party is responsible to the other Party for ensuring that the delivered services and the use of the Solution, respectively, comply with the relevant mandatory rules and regulations.

12.2 At the Customer's request, Visma is obligated to disclose Customer data and information on tasks performed on behalf of the Customer in accordance with the Agreement as requested by the authorities and/or the Customer's accountant.

13 LIMITATION OF LIABILITY

13.1 The Parties are liable in accordance with the general rules of Danish law, cf., however, clauses 13.1 and 14.

13.2 Neither of the Parties are liable for the other Party's indirect or consequential loss, including operating loss, loss of revenue, loss of profits or loss of goodwill.

13.3 The Customer is responsible for ensuring that documents signed through the Solution are valid and/or enforceable pursuant to applicable Danish or international legislation.

13.4 Visma is not liable for the punctuality of signatures or the emergence of documents generated through the Solution.

13.5 The Parties' total liability for loss and damage of any type may in no circumstance exceed the amount corresponding to the Customer's payments in accordance with the Agreement for the past 12 months calculated from the date the claim was raised.

13.6 The limitation of liability does not apply in case of a Party's gross negligence or intent.

14 FORCE MAJEURE

14.1 None of the Parties are liable to the other Party for circumstances outside the Party's control, and which the Party could neither have considered nor avoided or overcome at the conclusion of the Agreement.

15 ASSIGNMENT AND USE OF SUBSUPPLIERS

15.1 The Customer may not assign its rights and obligations pursuant to the Agreement to a third party without Visma's prior written accept.

15.2 Visma is entitled to use sub-suppliers as a part of the fulfilment of the Agreement.

16 BREACH

16.1 In case of a Party's material breach of the Agreement and if the breach has not been remedies no later than 10 days after the request of remedy from the non-breaching Party, the non-breaching Party is entitled to terminate the Agreement for cause without further notice. If the breach, due to its nature, cannot be remedies, the non-breaching Party may, however, terminate the Agreement for cause without a prior request for remedy.

16.2 In case of one Party's material breach, the general rules thereon of Danish law apply. A termination for cause will only have effect for the future (”ex nunc”).

17 DISPUTE RESOLUTION

17.1 Any disputes arising from the Agreement between the Customer and Visma regarding the Solution

must be settled in accordance with the rules of Danish law.

17.2 The venue for disputes (court of first instance) is the district court in the jurisdiction of Visma's registered office.

18 AMENDMENTS OF THE GENERAL TERMS AND CONDITIONS

18.1 Visma may amend these General Terms and Conditions with a written notice of 1 month. Any use of the Solution after the expiry of such notice constitutes an acceptance of the amended General Terms and Conditions.

APPENDIX 1. DATA PROCESSING AGREEMENT.

Between

The Data Controller: The Customer
Contact person: The person indicated as contact on the account

and

The Data Processor: Visma Consulting A/S, Nørgaardsvej 32, 2800 Lyngby, CVR.: 29973334
Contact person: addo@visma.com

Hereinafter referred to as the "Controller" and "Processor", a "Party" and collectively as the "Parties".

1. Introduction

1.1. Where the Controller uses the Solution and any module or function in connection with this (in its entirety called the "Solution"), the Processor will process personal data on behalf of the Controller.

1.2. With this data processing agreement (the "Agreement"), the Parties wish to establish their respective obligations and rights in relation to the processing of personal data in compliance with application legislation on the protection of personal data, which at the time of the Agreement's entry into effect includes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "GDPR") as well as any EU member state legislation supplementing the GDPR or otherwise setting out rules on processing of personal data to the extent applicable to the Parties (jointly the ”Data Protection Legislation”).

1.3. Both Parties confirm that the undersigned is authorized to enter into this data processing agreement (the "Agreement") on behalf of the Party concerned.

1.4. The Processor's processing of personal data is subject to Visma Group's Privacy Statement, which can be found at https://www.visma.com/privacy-statement/ and which applies to all companies in the Visma Group.

2. Definitions

2.1. In this Agreement, the terms "Personal Data", "Special Categories of Personal Data" (or "Sensitive Information"), "Processing", the "Data Subject", the "Data Controller" and "Data Processor" shall have the same meaning as in the Data Protection Legislation.

2.2. The Agreement has precedence in case of any conflict between the provisions on Processing of Personal Data in the Solution's General Terms and Conditions or other agreements entered into between the Parties. The Agreement is effective as long as the Controller subscribes to the Solution and the Processing in this connection processes Personal Data on behalf of the Controller. The Agreement does however not have precedence, if the Parties have entered into another data processing agreement, in which it is stated that that agreement has precedence to this Agreement.

3. The Controller's Obligations

3.1. Upon signing this Agreement, the Controller confirms that:

- The Controller will process Personal Data in compliance with the Data Protection Legislation when using the Solution.
- The Controller has the right to process and disclose the Personal Data to the Processor (and any sub-processors).
- The Controller has the sole responsibility of ensuring the accuracy, integrity, content, reliability and lawfulness of the Personal Data entrusted with the Processor.
- The Controller has fulfilled all obligations in relation to notification or receiving permission from the relevant supervisory authority with respect to the Processing of Personal Data.
- The Controller complies with its obligation to handle any Data Subject rights requests.
- The Controller does not process Sensitive Information when using the Solution, unless this is explicitly agreed in Sub-appendix A to this Agreement.
- The Controller will send an updated list of categories of Personal Data and Data Subjects, which is processed to the extent the Processing deviates from the description in Sub-appendix A.

4. The Data Controllers Instruction to the Data Processor

4.1. The Processor may only process Personal Data on behalf of and in accordance with the Controller's instruction. The General Terms and Conditions and this Agreement with appendices sets out the instruction at the time of signing, including that Processing of Personal Data must i) comply with applicable law and ii) only take place to the extent necessary to provide the services in accordance with the General Terms and Conditions, this Agreement and any other agreement entered into between the Parties. The Categories of Data Subjects and Personal Data that the Processor processes on behalf of the Controller are described in Sub-appendix A.

4.2. The Processor must notify the Controller if in the Processor's opinion any instruction is in violation of the Data Protection Legislation.

4.3. The Processor may only process Personal Data beyond the instruction if required by EU or EU member state law to which the Processor is subject. In case the Processing of Personal Data goes beyond the instruction, the Processor must inform the Controller, unless prohibited from doing so by EU or EU member state law.

5. Security of processing

5.1. The Processor must implement organisational and technical security measures to ensure that the Personal Data is subject to confidentiality, integrity and accessibility and is protected against any) accidental or unlawful destruction, loss or alteration, b) unauthorized disclosure of, access to, misuse of, or c) other unlawful processing or processing beyond the instruction.

5.2. At the time of signing, the Processor has implemented the technical and organisational security measures described in Sub-appendix B.

5.3. The Processor must without undue delay inform the Controller of any breach of security that has or could potentially lead to accidental or unlawful destruction, loss, alteration, unauthorized transmission of or access to the Personal Data processed on behalf of the Controller ("Security Breach").

5.4. The information must include a description of i) the nature of the Security Breach, including where possible the categories and approximate number of data subjects concerned as well as the categories of and approximate number of personal data records concerned, ii) the likely consequences of the Security Breach, and iii) the measures taken or proposed to be taken by the Processor to address the Security

Breach, including if relevant measures to minimize the potential harm.

5.5. The Processor must upon request assist the Controller in fulfilling its obligations to notify and inform the competent supervisory authority and/or Data Subjects. In case the Security Breach is not caused by the Processor, the Processor is entitled to payment based on the time spent and costs related to such assistance.

6. The Processor's Obligation to Assist the Controller

6.1. The Processor shall assist the Controller with appropriate technical and organisational measures to the extent possible and taking into account the nature of the Processing and the information available to the Processor in complying with the Controller's obligations in accordance with GDPR Article 32 to 36.

6.2. If the Processor receives a request from a Data Subject or a supervisory authority, the Processor must notify the Controller without undue delay. The Processor may not respond directly to any inquiries from the Data Subject, unless the Controller has authorized it. The Processor may only disclose Personal Data to public authorities, if the Processor is legally obligated to do so.

6.3. To the extent the assistance is not caused by the Processor's non-compliance with the Agreement and Data Protection Legislation, the Processor is entitled to payment for any assistance that supersedes the service which the Processor and/or Visma Group shall provide in consequence of the Data Protection Legislation.

7. Use of Sub-processors

7.1. As part of the provision of services the Processor uses sub-supplier ("Sub-processors"). Such Sub-processors may be other entities in the Visma Group or third party processors within or outside the EU/EEA. By signing this Agreement, the Controller provides the Processor with a general written authorization to use Sub-processors. At the time of signing, the Processor uses the in Sub-appendix C listed Sub-processors.

7.2. The Processor must inform the Controller of any intended changes concerning the addition or replacement of other Sub-processors and give the Controller the opportunity to object to such changes. The Controller may only object to such change if it has reasonable, specific reasons to do so. If the Parties cannot agree on the choice of a new Sub-processor, the Controller is entitled to unsubscribe from the Solution with effect before the new Sub-processor commences its Processing on behalf of the Processor.

7.3. Where the Processor uses a Sub-processor in connection with processing activities on behalf of the Controller, the same data protection obligations as those stated in this Agreement must be imposed on the Sub-processor, either by contract or another legal act guaranteeing in particular that the Sub-processor will implement appropriate organizational and technical measures to ensure that the Processing fulfils the requirements of the Agreement and the Data Protection Legislation.

7.4. The Processor remains fully liable to the Controller for the performance of the Sub-processors' obligations.

8. Transfers to Third Countries

8.1. The Processor may not cause or allow the transfer of Personal Data to countries outside the EU/EEA unless such transfer is included in the instruction or the Controller has given its prior written consent to such a transfer.

8.2. Insofar as the Controller has allowed a transfer in accordance with the above, the Processor must ensure that there is a legal basis for the transfer according to the Data Protection Legislation. By signing this Agreement, the Controller gives the Processor the authorization to enter into the EU Commissions

Standard Contractual Clauses on behalf of the Controller.

9. Demonstration of Compliance

9.1. The Processor must upon the Controller's request provide it with the necessary documentation enabling the Controller to ensure that the Processor fulfils i) it's obligations according to this Agreement, and ii) the provisions of the Data Protection Legislation in force at any given time, insofar as it concerns the Personal Data processed by the Processor on behalf of the Controller.

9.2. The Controller has the right to perform audits, including inspections at the Processors location to ensure that the Processor complies with its obligations. When sending a request for inspection to the Processor, the Controller must include a detailed plan on the extent, duration and time of the inspection no later than 4 weeks before the proposed date of commencement. If third parties are to carry through the inspection, this must be agreed upon between the Parties.

9.3. For security reasons, the Processor may however decide that the audit is to be carried out by a neutral third party of the Processor's choice, if the audit involves a processing environment where other controllers' data is processed.

9.4. If the proposed extent of the audit is similar to an ISAE, ISO or similar certification report carried out by a qualified third party auditor within the previous twelve months, and the Processor confirms that no material changes in the security measures subject to the audit have taken place in this period, the Controller must accept this audit report rather than request for an audit of the measures already covered by the report.

9.5. In any event the audit must take place within normal business hours at the relevant facility in accordance with the Processors policies and may not unreasonable disturb the Processors usual commercial activities.

9.6. The Controller bears own costs in connection with a requested audit. To the extent the Processor's assistance supersedes the service which the Processor or Visma Group must provide in consequence of the Data Protection Legislation, this will be charged separately.

10. Obligation of Confidentiality

10.1. The Processor must process Personal Data in confidence.

10.2. The Processor may not process, copy or disclose Personal Data, unless this is necessary to comply with the Processor's obligations and on condition that those to whom the Personal Data is disclosed are aware of the data's confidentiality and has accepted to keep it confidential in accordance with this Agreement.

10.3. The Processor must ensure that the persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10.4. The Processor's responsibilities in this section are not limited by nor contingent upon the Parties' continued or discontinued cooperation.

11. Duration and termination

11.1. The Agreement is effective as long as the Processor processes Personal Data on behalf of the Controller in connection with the Controller's use of the Solution.

11.2. The Agreement will automatically terminate at the end of the Controller's term of notice to subscription of the Solution. By termination of the subscription the Processor must delete or return all Personal Data in the relevant format in which the Processor has processed data on behalf of the Controller under the Agreement. If the Controller needs assistance in returning the data, costs in relation hereto are determined

jointly between the Parties and shall be based on:

i) hourly rates based on the Processor's time spent

ii) the complexity of the requested process, and

iii) the chosen format.

11.3. The Processor is entitled to keep the Personal Data after termination of the Agreement to the extent the Data Protection Legislation prescribes it. In such case, the continued Processing of the Personal Data will comply with the technical and organizational measures described in this Agreement.

12. Changes

12.1. Any changes to the Agreement shall be attached to this Agreement as a separate appendix.

12.2. If any of the provisions in the Agreement are invalid, it will not affect the remaining provisions. The Parties shall replace the invalid provision with a valid provision that reflects the purpose with the invalid provision.

13. Liability

13.1. Liability for actions in violation of this Agreement is regulated by the liability clause in the General Terms and Conditions. This also applies for any violation caused by a Sub-processor.

14. Applicable Law and Jurisdiction

14.1. This Agreement is subject to Danish law and any disputes shall be solved by the Danish courts.

SUB-APPENDIX A – CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

Categories of Data Subjects and Personal Data which may be subject to Processing under this Agreement

a. Categories of Data Subjects

i) The Controller's end-users

ii) The Controller's employees

iii) The Controller's contacts

iv) The Controller's customers and their end-users

v) The Controller's customers' employees

vi) The Controller's customers' contacts

b. Categories of Personal Data

i) Name

ii) Title

iii) Telefone number

iv) Email address

v) Address

Categories of Sensitive Information which may be processed under this Agreement

The Processor may on behalf of the Controller process one or several of the below indicated categories of Sensitive Information:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- Personal data relating to criminal convictions and offences
- CPR number
- Health information
- Data revealing a person's sex life or sexual orientation
- Data revealing trade union membership
- Genetic or biometric data for the purpose of uniquely identifying a natural person

SUB-APPENDIX B – DESCRIPTION OF SECURITY MEASURES

Introduction

This appendix describes the physical, technical and organizational security measures which the Processor ("Visma") as a minimum has implemented in accordance with the Main Contract and Agreement.

Services designed for security

From planning to deployment of new services or features, Visma follows its Security Development Lifecycle, which entails that security requirements are embedded and measured during development. Security requirements are based on a combination of sector and client-specific requirements as well as best practice, in compliance with privacy laws and regulations.

Visma performs security audits and penetration testing using both internal and external experts.

Visma's services are tested to ensure resilience against attacks such as SQLi, XSS and CSRF, session hijacking, and other threats. Visma's baseline is OWASP top 10.

The minimum security requirements that all development teams follow include:

- that passwords are never stored as text but are always "hashed and salted" server side, which entails that even Visma is unable to see a customer's password. If a password is lost, Visma will automatically generate a new one.
- that communication always takes place via an encrypted connection.

Visma stores personal data at Itadel (sub-processor)
Visma uses Itadel as a sub-processor to host and store all Personal Data. Itadel follows local European regulations and requirements regarding the protection of personal data and holds numerous certifications and declarations including ISO 27001, ISAE 3402 II and ISAE 3000.

For more information on Itadel, please click here: https://www.itadel.dk/en/

Monitoring and protection
Visma carefully monitors all services when making them available to the customers. This includes continuous scanning for vulnerabilities, monitoring of intrusion attempts as well as abuse detection.

Incident management

When incidents occur, Visma has a dedicated Security Incident Team that provides the necessary coordination, management, feedback and communication. The team is responsible for assessing, responding to and learning from information security incidents to make sure that Visma minimizes the risk of such incidents recurring.

Physical security

Visma has implemented several physical security measures, which include:

- 24 hour surveillance
- External and internal video monitoring and traceability of access to the premises
- Installed burglar alarms at relevant facilities
- Environmental control
- Uninterruptible power supply, which is regularly tested against fictional power outages

Access control

Visma protects all relevant facilities with burglar alarms. Only relevant employees will have access to Visma's facilities.

Access to the Controller's personal data is limited to a few employees who have a work-related need to access the information and who work with operations and technical support. Other employees will only gain access to the Controller's data when actively approved by the Controller.

Technical security

Firewalls and antivirus
Visma ensures that all machines and servers are equipped with antivirus software to block viruses, malware, etc. The network is protected by firewalls to ensure protection against unauthorized access.

Encryption
Visma ensures that Visma Addo follows industry standards. All external communication is encrypted using up to 2048 bit.

Communication from Itadel
All communication from Itadel to external parties is encrypted using X.509 certificates, which is a standard for Public Key Infrastructure (PKI) issued by an authorized organization called Certificate Authority (CA), which is responsible for confirmation of identity. The certificate contains two keys for asymmetric encryption, a public key and a private key. Only the certificate owner has access to the private key used for encryption. The encrypted content can be decrypted only with the matching public key. By relying on the certificate issuer, the sender’s identity is ensured and thus the content. Visma Addo supports the newest and securest encryption and is committed to updating it when essential. Currently, Visma Addo supports TLS v. 1.2

Communication with third-party suppliers
All communication with Nets and e-Boks is secured using a VOCES certificate issued by Nets. VOCES is a merchant certificate that represents a business, in this particular case, Visma. The VOCES is used to secure communication between different parties. Visma Addo supports the newest and securest encryption and is committed to updating it when essential. Currently, Visma Addo supports TLS v. 1.2

Emails
Delivery of e-mails to a recipient requires encryption of attachments as they may contain sensitive personal information. The attached documents are encrypted up to 2048-bit AES (Advanced Encryption Standard).

Logging
Visma logs all access to the services with the purpose of tracing activity and documenting all events in the system. The logging registers the time of access and which employee has accessed the data.

Deletion and discarding

IT storage
Hard drives and other storing media that are discarded from the operation are destroyed in a way that makes it impossible to restore the data. All reused discs are formatted in accordance with applicable industry standards.

Storage of data and backup
Visma regularly carries out a security backup of personal data stored in the system. Backups are stored separately and securely so that the personal data can be restored. Instructions on the deletion of personal data include the deletion of personal data in backups.

Organizational security

Access rights
Visma ensures that employees only have access to the systems where relevant in order for them to perform their tasks. All employees are bound by Visma's guidelines and rules when accessing and processing personal data and are monitored when accessing client-specific information.

All employees have a unique user name and password. User names and passwords are created and changed according to generally accepted principles. All rejected access attempts are registered. After repeatedly rejected access attempts from the same workstation or with the same user identification, further access attempts are blocked. Successful and unsuccessful access attempts are handled by SIEM (security information and event management).

Confidentiality
All employees at Visma who have access to personal data are covered by confidentiality agreements.

Technical Security Surrounding the Signature in Visma Addo

At Visma our first priority is security. People choose digital signatures for being the most secure type of electronic signature. Digital signatures differ from a normal handwritten signature, as digital signatures provide the highest level of assurance with regard to the signers' identity and the authenticity of the documents signed.

In order to be valid, either digitally or physically, a signature must meet three basic requirements:

1. Signer authentication
2. Content integrity
3. Non-repudiation

Signer authentication
This requirement stipulates that Visma must have security for the signer's identity. Visma provides different authentication methods, such as NemID, SMS code or SITHS to authenticate the signer's identity and demonstrate proof of signing. To further increase security, when a customer uses NemID, the unique PID (Personal Identifier) is also printed on the document, assuring that the signer's certificate is cryptographically bound to the document.

The signed document will always be blocked from further changes regardless of the signing method and is supplied with a timestamp with a certificate from GlobalSign. All cryptographically signing proofs are embedded in the PDF, enabling all parties to validate the signing in the future. In Norway and Sweden, BankID is the most widely used solution, and in Denmark, NemID is the most secure way of assigning a digital signature to a physical person. These signing methods are all supported by Visma Addo.

Content integrity
Visma Addo is designed to keep the customer's documents secure and to prevent tampering with the documents. If the document changes after signing, the digital signature is invalidated and the one who opens the document is notified. When a document is signed, a unique Visma Addo identification number is printed on the document and a "checksum" is created based on the document content including the unique identification number.

Non-repudiation
Non-repudiation can be achieved using one or several of the official public signatures (NemID, BankID, etc.) - either signing directly with a public signature or in combination with other forms of signatures in Visma Addo.

SUB-APPENDIX C – LIST OF SUB-PROCESSORS

At the time of signing this Agreement, the Processor's sub-processors with access to the Controller's Personal Data include:

Name	Country	Legal basis for transfer to third country	Type of service
Itadel A/S	Denmark	N/A	Hosting