GENERAL TERMS AND CONDITIONS FOR ADDO SIGN

VERSION 5.0, SEPTEMBER 2023

1 INTRODUCTION

1.1 These subscription terms and conditions (the "Terms") apply to twoday A/S, Gærtorvet 1-5, 1799 Copenhagen V, business reg. no.: 29973334 ("twoday") and the customer as identified in the order form or otherwise (the "Customer" or "You"). If the Customer is a legal person, the Terms are accepted on behalf of the Customer.

1.2 BY REGISTERING FOR, ACCESSING, BROWSING, AND/OR OTHERWISE USING ADDO SIGN, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND ACCEPT TO BE BOUND BY THESE TERMS. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS, DO NOT ACCESS, BROWSE OR OTHERWISE USE ADDO SIGN. YOUR ACCEPTANCE INCLUDES THE DATA PROCESSING AGREEMENT IN APPENDIX 1.

1.3 The Terms stipulate the Parties' rights and obligations in connection with the Customer's use of the digital signing solution, Addo Sign (the "Solution").

1.4 The original language of these Terms is English. twoday may make available translations for convenience. In case of conflicts between the original English version and any translation, the English version shall prevail.

1.5 The Solution is intended for businesses and authorities (as opposed to consumers).

2 DEFINITIONS

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 Terms, cf. Clause 1.2.

2.1.2 The "**Customer**": The business or authority using the Solution, cf. Clause 1.1.

2.1.3 The "**Data Processing Agreement**" or the "**DPA**": Has the meaning set out in Clause 10.1

2.1.4 The "**Solution**": twoday's digital signature solution, cf. Clause 1.3. See a detailed description of the Solution at **www.addosign.com.**

2.1.5 The "**Party**"/"**Parties**": The Customer and/or twoday according to the context.

2.1.6 The "**Terms** ": These general terms and conditions for the Solution, cf. Clause 1.1.

2.1.7 "**Account**": The primary means for accessing and using Solution subject to payment of a Subscription Fee set out in the selected Plan.

2.1.8 **"Plans**": Various criteria related to the use and functionality of the Solution and on which the Subscription Fee is based.

2.1.9 "**Subscription Fee**": The regular payment for using the activated Account.

2.1.10 "**Billing Cycle"**: A Billing Cycle, is the interval of time between invoices under a specific Plan. Billing Cycles may vary in length depending on the chosen Plan. Typically, the Billing Cycle is either one (1) month or twelve (12) months.

2.1.11 "**Transaction**": A Transaction is composed by one or several of the following steps:

- Notification: Notification to the receiver on the receipt of one or more documents to be signed or otherwise handled.
- Identification: The option of requiring identification from the recipient before signing or otherwise handled.

- Signing: The recipient can sign documents with the signing options available in the Solution
- Distribution: The option to distribute documents/data through the channels available in the Solution

2.1.12 "**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 twoday has in connection with the individual Transaction.

2.1.13 **Working days:** Monday – Friday except public holidays in Denmark.

3 THE CUSTOMER'S USER RIGHTS

3.1 twoday owns all rights in 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 Terms.

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

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

3.2.3 Any use of the Solution by the Customer's affiliates is subject to these Terms and the Customer is responsible towards twoday for any such use.

3.2.4 The Solution can be accessed and used by using a username and password.

3.2.5 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.

3.2.6 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, cf. Clause 2.1.1, and the twoday has created an Account.

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 twoday with a notice of six (6) months to the end of a calendar month.

4.4 If the Agreement is terminated, 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 FEES/PAYMENT

5.1 The prices applicable always appear on the Solutions country websites The prices are listed in local currency exclusive of VAT (Value Added Taxes). Upon at least one month's prior notice to the Customer, we reserve the right to change the composition, content and prices of products and subscriptions with notice by e-mail or by posting on our websites.

5.2 Customers may cancel their Plan anytime as outlined below, however must do so prior to the renewal Date in order to avoid billing of the next Plan Term's Fees. The Customer authorizes twoday to automatically charge The Customer the applicable Fees on or after the renewal Date unless the Plan has been terminated or cancelled in accordance with these Terms.

5.3 If the Customer chooses to cancel its Plan during the Plan Term, the Customer may use the Solution

until the end of Customer's then-current Plan's Billing Cycle but will not be issued a refund for the most recently (or any previously) charged Fees. Except for the exceptions described in section 6.2.4 Fees for purchased Credits cannot be refunded in any circumstances, including when the Agreement expires.

5.4 Invoices are due for payment 20 days after the invoice date. Interests of 2 per cent per month will accrue on late payments.

5.5 If the Customer does not pay an outstanding fee regarding the Solution, despite a prior written claim for payment of minimum 10 days, twoday is entitled to close the Customer's access to the Solution until payment is made and/or at twoday's discretion terminate the Agreement without further notice.

6 PLANS

6.1 The Customer may choose various payment models for the use of the Solution ("Plans") as described in this Clause.

6.2 **Plan – "Starter".** This Plan is based on a "pay as you go" principle with no fixed Subscription Fee**.** The Customer can therefore buy Credits on an ongoing basis. The fee for additional Credits, volume discounts and prices of the individual transaction types are listed on **www.addosign.com.**

6.2.1 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. The fee is deducted from the Customer's account at the same time Credits are added to the Customer's Account.

6.2.2 If the Customer has not purchased Credits for 12 consecutive months, any unused Credits will expire. The period of expiry always applies from the date of the latest purchase of Credits. The Customer's administrator will receive notification of this in the Solution thirty (30) and five (5) days before expiry. If the Customer has not used the Solution for 6 consecutive months after the expiry of the Credits, the Account will be deleted.

6.2.3 Selected add-ons/modules or services are invoiced with a monthly Billing Cycle and can be terminated by the Customer to the end of Billing Cycle (apart from the optional service agreement where the Customer's minimum commitment is 3 months)

6.2.4 If the Customer wishes to switch from Plan "Starter" to a Plan "Addo 10-500", the Supplier offers to buy back the Customer's excess credits. The price per credit is listed on the Solutions country websites. The total price for redeeming Credits can never exceed the Customer's payment for the first Billing cycle for the selected Plan.

6.3 **Plan - "Addo 10-500".** This Plans for using the Solution with either be based on a monthly or an annual subscription period/Billing Cycle.

6.3.1 The Customer has the right to upgrade or downgrade a current Plan at any time by selecting a new Plan from the collection of Plans determined by the Supplier. In such an event the Supplier will automatically be charged with a fee for the next payment interval with the rate stipulated in the new Plan.

6.3.2 Upgrading Plans: If the Customer is upgrading Plans, the new Plan will apply immediately, and the Customer will receive a credit note and an invoice. The credit note will be for the balance remaining in the current period of the original Plan. The Customer will then receive an invoice charging for the new Plan for the remainder of the Billing Cycle. The balance of the credit note will be applied fully to the invoice for the new Plan. Any consumption of Credits in excess of the contained number of Credits in the original Plan will be invoiced when switching to a new Plan.

6.3.3 Downgrading Plans: If the Customer is downgrading Plans, the changes will take effect at the beginning of the next Billing Cycle, when the next renewal invoice is issued. Further, subscription changes made before the end of the current Billing Cycle may override the

scheduled one. Downgrading of the Current Plan may cause the loss of features, functionality, or capacity of the Account, as well as loss of the Customer's data.

6.3.4 The Agreement can be terminated by Customer to the end of a Billing Cycle

6.3.5 Billing of selected add-ons/modules or services follows the Billing Cycling on the selected Plan. Subscription of modules/services can be terminated individually at the end of a Billing Cycle (apart from the optional service agreement where the Customer's minimum commitment is 3 months).

6.3.6 If the Customer with an annual Plan has an excess consumption of credits that exceeds the number of credits in the selected plan by more than 500%, the Supplier has the option of billing the excess number of credits monthly for the remainder of the Billing Cycle.

7 OPERATION AND MAINTENANCE

7.1 twoday is obligated to ensure a stable and continuous operation of the Solution, including ongoing maintenance by correcting errors and inconveniences.

7.2 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, twoday is entitled to close down all or part of the Solution outside the stated maintenance period.

7.3 Based on the Customer's inquiries and twoday's own monitoring of the Solution, twoday will perform error correction of the Solution.

7.4 twoday 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. Preventive maintenance will not be performed within the period 08.00 – 18.00 on Working Days.

8 CHANGES

8.1 twoday is entitled to make ongoing updates and improvements to the Solution. twoday 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.

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

9 SUPPORT

9.1 The Customer can request support of the Solution during the period 8.30-17.00 CET on Addo Signs website under "Support".

10 PERSONAL DATA AND SECURITY

10.1 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 twoday 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 twoday's processing of the Customer's personal data, including the Customer's instructions to twoday regarding the processing of personal data on behalf of the Customer.

10.2 The Customer's data is processed and stored securely and twoday 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.

10.3 twoday 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.

11 CONFIDENTIALITY

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

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

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

11.4 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 twoday hereof.

12 RENTENTION OF DATA AND BACK-UP

12.1 Documents will be stored for 10 days in the Solution after which it is automatically deleted (Unless the Customer has activated the Solution's ability to archive documents). Other data regarding the Transaction will not be deleted. The Customer has the option to anonymize data

12.2 twoday performs a daily backup of the Solution and the Customer's data. The back-up is stored for 30 days. twoday is responsible for ensuring that backup copies are stored securely.

13 LEGAL AND REGULATORY REQUIREMENTS

13.1 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.

13.2 At the Customer's request, twoday 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.

14 LIMITATION OF LIABILITY

14.1 The Parties are liable in accordance with the general rules of Danish law, cf., however, clauses 13.2 and 14.

14.2 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.

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

14.4 twoday is not liable for the punctuality of signatures or the emergence of documents generated through the Solution.

14.5 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.

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

15 FORCE MAJEURE

15.1 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.

16 ASSIGNMENT AND USE OF SUBSUPPLIERS

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

16.2 twoday is entitled to use sub-suppliers as a part of the fulfilment of the Agreement.

17 BREACH

17.1 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 remedied, the non-breaching Party may, however, terminate the Agreement for cause without a prior request for remedy

17.2 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”). DISPUTE RESOLUTION

17.3 Any disputes arising from the Agreement between the Customer and twoday regarding the Solution must be settled in accordance with the rules of Danish law.

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

18 AMENDMENTS OF THE GENERAL TERMS AND CONDITIONS

18.1 twoday may amend these Terms with a written notice of one (1) month provided, however, that in case of material amendments, the Customer has the right to terminate the Agreement with a notice of 20 days after receipt of the notice. Any use of the Solution after the expiry of such notice constitutes an acceptance of amendments of the Terms and a waiver of the Customer’s right to terminate the Agreement due to such amendments.

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: twoday A/S, Gærtorvet 1-5, 1799 Copenhagen V, CVR.: 29973334
Contact person: support@addosign.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 "**DPA**"), 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 DPA'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 their representative entering into the Agreement (inclusive this DPA) is authorized to enter into this DPA on behalf of the Party concerned.

2. Definitions

2.1. In this DPA, the terms "**Personal Data**", "**Special Categories of Personal Data**", "**Processing**", the "**Data Subjec**t", the "**(Data) Controller**" and the "**(Data) Processor**" shall have the same meaning as in the Data Protection Legislation.

2.2. The DPA has precedence in case of any conflict between the provisions on Processing of Personal Data in the Terms or other agreements entered into between the Parties.

2.3. The DPA applies as long as the Controller has access to the Solution and the Processor processes Personal Data on behalf of the Controller.

3. The Controller's Obligations

3.1. Upon entering into of the 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 complies with its obligation to handle any Data Subject rights requests.
- The Controller does not process Special Categories of Personal Data when using the Solution, unless this is agreed in Sub-appendix A to the Agreement.
- The Controller will send the Processor 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 Controller's 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. At the entering into of the Agreement, the said instruction is to Process such Personal Data on behalf of the Controller which is needed for the Processor's delivery of the services to the Controller as set out in the Agreement, including digital signing, document generation, storage of signed documents and identification of the signer. 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 immediately 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 about the Security Breach. In case the Security Breach is not caused by the Processor, the Processor is entitled to payment for its assistance with handling the Security Breach 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 to do so. 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 DPA and Data Protection Legislation, the Processor is entitled to payment for any assistance to the Controller under this DPA.

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 twoday Group or third-party processors within or outside the EU/EEA. By signing the Agreement, the Controller provides the Processor with an authorization to use Sub-processors as set out in Sub-appendix C.

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 Controller has objections to a new Sub-processor, the Controller sole and exclusion option is 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 the DPA 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 DPA 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. In case of any transfers of Personal Data to third countries (i.e., countries outside of EU/EEA), the Processor must ensure that there is a legal basis for the transfer according to the Data Protection Legislation.

8.2. The Controller instructs the Processor to transfer Personal Data to any of the countries listed in Sub-appendix C.

9. Demonstration of Compliance

9.1. The Processor must upon the Controller's request provide the Controller with the necessary documentation enabling the Controller to ensure that the Processor fulfils i) it's obligations according to this DPA, 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 Processor's location to ensure that the Processor complies with its obligations. When requesting an inspection, the Controller must include a detailed description of the extent, duration and time of the inspection no later than 4 weeks before the proposed date of commencement of the inspection.

9.3. For security reasons, the Processor may 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' Personal 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 show good reasons for requesting 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 Processor's policies and may not unreasonably disturb the Processor's usual commercial activities.

9.6. The Controller bears own costs in connection with a requested audit. The Processor's assistance in connection with the audit will be charged the Controller separately on a time & material basis unless the audit identifies a breach of the DPA by the Processor.

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 the DPA.

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 DPA 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.

The Agreement will automatically terminate at the end of the Controller's term of notice to unsubscribe from the Solution. By termination of the subscription, the Processor must delete or return to the Controller all Personal Data in the relevant format in which the Processor has processed data on behalf of the Controller under the DPA. If the Controller needs assistance in returning the data, the Processor will charge the Controller for such assistance on a time & material basis.

11.2. Notwithstanding the foregoing, the Processor is entitled to keep the Personal Data after termination of the DPA 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 the DPA.

12. Changes

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

12.2. If any of the provisions in the DPA 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 the DPA is subject to the limitation of liability clause in the Terms. This also applies for any violation caused by a Sub-processor.

14. Applicable Law and Jurisdiction

14.1. The DPA 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

A.1 The purpose of the Processor's processing of personal data on behalf of the Controller:

The purpose of the processing is to provide the Controller with a digital signature solution enabling users to sign, send and manage documents and validate the identity of the users.

A.2 The Processor's processing of personal data on behalf of the Controller shall mainly pertain to the following (nature of the processing):

To manage and host a platform (the Solution) where users can upload documents for electronical signing. The users upload documents at their own discretion and the Processor stores the documents for 10 days after complete signing or for another time-period agreed with the Controller.

A.3 Categories of Data Subjects and Personal Data which may be subject to Processing under the 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. Types of Personal Data

i) Name

ii) Title

iii) Telephone number

iv) Email address

v) Address

iv) Personal identification number (in Denmark: CPR-number)

Special Categories of Personal Data which may be processed under the DPA

The Processor may on behalf of the Controller process one or several of the below indicated Special Categories of Personal Data depending on the Controller's actual use of the Solution:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- Personal data relating to criminal convictions and offences
- 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 Sub-appendix describes the physical, technical and organizational security measures which the Processor (herein also referred to as twoday) as a minimum has implemented in accordance with the DPA.

Services designed for security

From planning to deployment of new services or features, twoday 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.

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

twoday's services are tested to ensure resilience against attacks such as SQLi, XSS and CSRF, session hijacking, and other threats. twoday'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 twoday is unable to see a customer's password, if a password is lost, twoday will automatically generate a new one.
- that communication always takes place via an encrypted connection.

twoday stores personal data at IT Relation and Cloud Factory (sub-processor)

twoday uses IT Relation and Cloud Factory as a sub-processors to host and store all Personal Data. IT Relation and Cloud Factory follow 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 IT Relation, please click here: https://www.it-relation.com
For more information on Cloud Factory, please click here: https://www.cloudfactory.dk/

Monitoring and protection

twoday 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, twoday 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 twoday minimizes the risk of such incidents recurring.

Physical security

twoday 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
twoday protects all relevant facilities with burglar alarms. Only relevant employees will have access to twoday'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 Personal Data when actively approved by the Controller.

Technical security

Firewalls and antivirus
twoday 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
twoday ensures that Addo Sign (the Solution) follows industry standards. All external communication is encrypted using up to 2048 bit.

Communication from IT Relation and Cloud Factory
All communication from IT Relation and Cloud Factory 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. Addo Sign (the Solution) supports the newest and securest encryption and is committed to updating it when essential. Currently, Addo Sign (the Solution) 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, twoday. VOCES is used to secure communication between different parties. Addo Sign (the Solution) supports the newest and securest encryption and is committed to updating it when essential. Currently, Addo Sign (the Solution) 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
twoday 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 Customer’s Personal 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
twoday regularly carries out a security backup of Personal Data stored in the Solution. 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
twoday ensures that employees only have access to the Solution where relevant in order for them to perform their tasks. All employees are bound by twoday's guidelines and rules when accessing and processing Personal Data and are monitored when accessing client-specific information.

All employees have a unique username and password. Usernames 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 twoday who have access to Personal Data are covered by confidentiality agreements.

Technical Security Surrounding the Signature in Addo Sign

At twoday 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 twoday must have security for the signer's identity. twoday 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 Addo Sign (the Solution).

Content integrity
Addo Sign (the Solution) is designed to keep the customers' 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 Addo Sign 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 Addo Sign (the Solution).

SUB-APPENDIX C – LIST OF SUB-PROCESSORS

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

Name	**Address**	**Legal basis for transfer to third country**	**Type of service/processing**
IT Relation A/S	Nygårdsvej 5A, 2., Copenhagen, Denmark	N/A	Hosting including storing of Personal Data included in the Solution
Cloud Factory A/S	Vestergade 4, 6800 Varde, Denmark	N/A	Hosting including storing of Personal Data included in the Solution
SendGrid, Inc.	375 Beale Street Suite 300 San Francisco, CA 94105 USA	EU-U.S. Data Privacy Framework	E-mail supplier E-mail sending and distribution
COMPAYA A/S	Palægade 4, 2. 1261, Copenhagen, Denmark	N/A	SMS-supplier SMS sending and distribution