GENERAL TERMS AND CONDITIONS FOR ADDO SIGN
VERSION 7.0, OCTOBER 2025

1 INTRODUCTION

1.1 These subscription terms and conditions (the "Terms") apply to twoday A/S, Sundkaj 125, 2150 Nordhavn, 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 the Solutions country websites.

6.2.1 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.

6.2.2 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)

6.2.3 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 RETENTION OF DATA AND BACK-UP

12.1 The Solution retains documents for forty (40) days after they have been signed by all designated parties. The documents is automatically deleted if the signing period expires or if the document is declined by a designated signer (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. The data controller may modify the retention period within the Solution.

12.2 User profiles will be deactivated twelve (12) months after the termination of the Solution or the last recorded purchase of credits. Once deactivated, profiles will be retained for an additional six (6) months before being permanently deleted from the Solution.

12.3 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”).

18 DISPUTE RESOLUTION

18.1 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.

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

19 AMENDMENTS OF THE GENERAL TERMS AND CONDITIONS

19.1 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

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The Customer
(the data controller)

and

twoday Danmark A/S
CVR 29 97 33 34
Sundkaj 125
2150 Nordhavn
Denmark
(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Indholdsfortegnelse

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In relation to the provision of the data processor's digital signing solution, Addo Sign (the "Solution"), the data processor will process personal data on behalf of the data controller in accordance with the provisions outlined in the Clauses. The Solution enables the data controller to digitally sign, send and manage documents while validating the identities of individuals digitally signing documents through the Solution.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Sub-Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Sub-Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Sub-Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Sub-Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with sub-appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in sub-appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State[1] data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Sub-Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least sixty (60) days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Sub-Appendix B. The list of sub-processors already authorised by the data controller can be found in Sub-Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against

the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Sub-Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

    a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller's obligation to without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

    c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Sub-Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within twenty-four (24) hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9.2.a., the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Sub-Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in sub-appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of the data controller's acceptance of the Clauses during the registration process for the Solution.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the

Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Sub-Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Acceptance of the Clauses
   The data controller and data processor acknowledge and accept that the Clauses shall become binding upon the data controller's registration for the Solution, and such acceptance will carry the same enforceability as a signature.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   The data controller can be contacted using the information provided in their account within the Solution.

   The data processor can be contacted via e-mail at: support@addosign.com.

Sub-Appendix A (Information about the processing)

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the processing is to provide the Solution to the data controller as outlined in Clause 2.3.

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

In accordance with Clause 2.3., and as instructed by the data controller, the nature of the data processor's processing entails the storage of documents and personal data uploaded to the Solution by the data controller. Additionally, the data processor will transmit documents to recipients for digital signing, as instructed by the data controller.

A.3. The processing includes the following types of personal data about data subjects:

The processing will include the following types of personal data, cf. GDPR article 6:

- Name
- Title
- Telephone number
- Email address
- Personal identification number
- Address

The data processor may on behalf of the data controller process one or several of the below indicated **special categories of personal data** ("sensitive personal data"), cf. GDPR article 9:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

The parties acknowledge and agree that the data processor may, as part of its processing on behalf of the data controller, process personal data that, according to the Danish Data Protection Act (in Danish, "Databeskyttelsesloven"), requires the same legal basis as the processing of personal data listed in GDPR Article 9. This includes data subjects' personal identification numbers, cf. the Danish Data Protection Act § 11(2)(4), cf. § 7(1), and information related to data subjects' criminal offenses, cf. the Danish Data Protection Act § 8(3).

A.4. Processing includes the following categories of data subject:

The processing will include the following categories of data subjects:

- The data controller's users
- The data controller's customers' users

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The duration of the data processor processing of personal data on behalf of the data controller shall be in accordance with the retention policy for personal data, as specified in Sub-Appendix C, Clause C.4.

Sub-Appendix B (Authorised sub-processors)

B.1. Approved sub-processors
On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
team.blue Denmark A/S	29 41 20 06	Højvangen 4, 8660 Skanderborg, Denmark	Hosting and storage of personal data.
Retarus GmbH	HRB 101134	Aschauer Straße 30, 81549 München, Germany	Sending and distribution of email messages generated through the Solution.
COMPAYA A/S	31 37 54 28	Palægade 4, 2. 1261, Copenhagen, Denmark	Sending and distribution of SMS messages generated through the Solution.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors
The data processor shall inform in writing to the data controller (at least sixty (60) days in advance) of any intended changes concerning the addition or replacement of sub-processors, cf. Clause 7.3., thereby giving the data controller the opportunity to object to such changes.

However, the data controller may only object to the use of a sub-processor if such use will constitute a violation of the data controller's obligations under applicable EU or Member State law. The data processor must receive the data controller's written objection no later than twenty-one (21) days from the data processor's notification to the data controller. If the data processor does not receive such objection, the data controller shall be deemed to have authorised the use of the sub-processor.

Sub-Appendix C (Instruction pertaining to the use of personal data)

C.1. The subject of/instruction for the processing
The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor shall carry out processing activities deemed necessary for the purpose of fulfilling its obligations pursuant to Clause 2.3. and as instructed in writing by the data controller.

C.2. Security of processing
The data processor shall be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed upon) level of data security.
The data processor has implemented the following systematic, organizational, and technical measures to ensure an appropriate level of security, considering the technology and the costs of implementation in relation to the risks involved, as well as the nature of the personal data to be protected.

- The data processor ensures a high level of security in its products and services (whether or not the processing involves personal data subject to Article 9 GDPR "special categories of personal data"), in accordance with the requirements for information security outlined in the General Data Protection Regulation, Article 32.

- The data processor's internal framework for safeguarding the data controller's personal data is designed to guarantee the confidentiality, integrity, and availability of personal data. Key measures within this framework include:

Risk management

- The data processor must establish and maintain a risk management process that is proportionate to the risks arising from the processing activities under these Clauses, taking into account the nature, scope, context, and purposes of the processing, as well as the risks likely to result from the processing in the ordinary, reasonably foreseeable and intended use of the Solution.

- The data processor shall provide risk mitigation and monitoring of risks to ensure that risk management is appropriate for the nature and scope of the Solution outlined in Clause 2.3. and compliant with recognised industry standards.

- The data processor shall maintain appropriate levels of industry standards and best practices, methodology and technology knowledge and fulfil security controls for the Solution in line with the data processor's implemented security framework, which is aligned with recognised industry standards (e.g. ISAE 3000/ISAE 3402), and appropriate for the level of risk associated with the Solution outlined in Clause 2.3.

Human resources

- In particular, as required by GDPR or applicable EU or Member State data protection provisions, the Supplier will:
  - take reasonable steps to ensure the reliability of all personnel of the data processor and/or the data processor's sub-processors who processes personal data under the Clauses.
  - ensure that all personnel of the data processor and/or the data processor's sub-processors processing personal data are informed of the confidential nature of the personal data and have committed themselves to the obligation of confidentiality, cf. Clause 5.1. or are under a statutory obligation of confidentiality.
  - ensure that all personnel of the data processor and/or it's sub-processors processing personal data shall have received awareness and security training relevant to their respective roles.

Asset management

- The data processor shall have an asset management policy and maintain an inventory of all assets holding personal data including hardware, software, electronic documents and physical documents/media.

Physical and environmental security

- Physical access to areas where personal data are processed shall be protected by the following requirements:
  - Access only to identified authorized individuals.
  - All access to the production area shall be logged.
  - Cameras and alarms must be located in relevant areas of the datacentres e.g. entries to datacentres.
  - The area must employ a proximity access control system, e.g. access cards, to secure the data processor's equipment and other equipment used for processing personal data.

Environmental controls

- Following environmental controls shall be in place:

- Fire protection and suppression:
  Fire extinguishers, alarms, and emergency buttons shall be installed to protect the facilities and IT systems.

- Uninterruptible Power Supply ("UPS"):
  UPS shall be installed on the data processors network and servers to protect the facility and computer equipment from electrical power fluctuations and outages.

Access control

- The data processor shall maintain a record of security privileges of personnel having access to personal data.

- The data processor's access to personal data shall be restricted to authorised personnel only and granted access rights must be based on a strict need-to-know and least-privilege principle.

- The data processor shall review access rights at regular intervals, at least annually, or in accordance with the data processor's internal access management policy validating access and removing access to personal data, physical locations, equipment and programs for those individuals who no longer have a business need and/or are no longer authorised by the data processor to have access.

Authentication

- The data processor shall use industry standard practices to identify and authenticate users who attempt to access information systems.

- Where authentication mechanisms are based on passwords:
  - passwords shall be renewed regularly.

  - password shall be at least eight characters long, contain numeric characters, and password history restrictions must be established.

  - repeated attempts to gain access to the information system using an invalid password shall be monitored and appropriate action shall be taken in the case of suspected attempts of abuse.

  - procedures shall be in place to deactivate passwords that have been corrupted or inadvertently disclosed.

- password must be protected in order to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

- Access to personal data processed on behalf of the data controller is logged.

- Access to production data, which may include sensitive personal data, is permitted only through a VPN connection with two-factor authentication. Each access request to production data is evaluated on a case-by-case basis.

System development and maintenance

- The data processor shall follow best practices for secure programming in relation to software applications.

- All changes to production systems shall be quality assured and follow a formal and documented change management procedure.

- The data processor shall have a process for the adoption, testing, and deployment of patches relevant for the systems related to the services provided to the data controller.

- The data processor shall conduct regular vulnerability assessments, including penetration testing with the baseline set to the OWASP top 10.

Technical measures

- The data processor must ensure the following technical measures have been established:

  - Control environment:
    Documented control environment and ensuring segregation of duties where necessary.

  - Anti-virus:
    Active anti-malware controls on all relevant servers and end user devices with an up-to-date signature file.

  - Firewalls:
    Firewalls to isolate the production data from the public internet and other unsecure zones.

  - DDoS:
    Appropriate levels of protection against DDoS attacks must be implemented.

  - Data backup and recovery:

Regular security backups of the personal data are performed and stored separately for thirty (30) days.

- Bulk transfers:
  Systems holding personal data must have mechanisms to protect against risks of unauthorised downloading of bulk data.

- Encryption:
  Personal data is encrypted in transit over public networks using encryption protocols up to 2048 bits. Personal data at rest, including but not limited to data stored on servers, workstations, mobile devices, and removable media, is also encrypted to ensure data security.

- Segregation of data:
  Personal data is logically or physically segregated from the data of other customers of the data processor, ensuring data isolation and protection against unauthorized access.

- Logging:
  - System log:
    System logs are maintained exclusively for the purposes of diagnostics, performance monitoring, and system troubleshooting the Solution. They record system-level technical events and operations. Typical entries may include system errors, background processes, and performance metrics.
    Access to system logs is restricted to a limited group of authorized employees who are granted access strictly in case of troubleshooting and system optimization. System logs are retained only for the period necessary to fulfil the purposes outlined above.

  - Audit log:
    Audit logs constitute a structured and time-stamped record of user profile actions performed within the Solution. They serve as a critical control for security, accountability, and compliance with data protection obligations, and may include information such as data modifications, deletions, and administrative actions.
    Audit logs are retained for the duration of the user profile's active subscription unless the user profile enables the Solution's anonymization functionality, in which case audit logs will be deleted.

Remote work

- Access to personal data from remote work locations shall be subject to the same security measures and access controls that apply to workplaces at the data processor's premises.

Destruction of data

- The data processor shall use industry standard processes to delete personal data when it is no longer needed or upon request from the data controller, cf. Clause 11.1.

Business continuity

- The data processor must have an up-to-date disaster recovery and business continuity plan in place for their systems relevant for the Solution outlined in Clause 2.3.

- The business continuity plan shall be regularly tested by the data processor or by a third party appointed by the data processor to ensure ongoing operational resilience.

- The performed testing of the business continuity plan must be documented and any findings and lessons learned during tests must be used for continuous improvement of plans.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- The data processor must - within the time limit set forth in Clause 10.2. - assist the data controller with all available information in the event of a data breach, in order for the data controller to assess the extent of the breach, so the data controller is able to report the breach to the relevant Data Protection Agency and notify relevant data subjects.

- The data processor must without undue delay, inform the data controller in writing of any request addressed to the data processor by a data subject to exercise the data subjects' rights related to the data processor's processing activities. The data processor shall not be entitled to respond to such requests unless instructed to do so by the data controller.

C.4. Storage period/erasure procedures

The storage period of personal data processed under these Clauses varies depending on the specific processing activities carried out to fulfil the purpose described in Clause A.1. of Appendix A.

<u>Transaction data:</u>

Transaction data refers to personal data included in the metadata associated with the signing workflow, including, but not limited to, the names, email addresses, and telephone numbers

of the involved parties. Such personal data will be processed for as long as the user profile associated with the transaction data remains active within the Solution and will be deleted concurrently with the deletion of the associated user profile. The data controller may anonymise transaction data at any time following the completion of the associated transaction.

Documents:
Personal data may be contained within documents uploaded to the Solution for the purpose of signing workflows. Such documents shall be retained within the Solution for a period of forty (40) days following full execution by all designated signatories. In cases where the signing period expires without completion or where a document is explicitly declined by any designated signer, the document will be automatically deleted from the Solution. The data controller may modify the retention period for documents within the Solution.

User profiles:
User profiles will be deactivated twelve (12) months after the termination of the subscription to the Solution or the last recorded purchase of credits. Once deactivated, user profiles will be retained for an additional six (6) months before being permanently deleted from the Solution.

C.5. Processing location
Processing of the personal data under the Clauses cannot be performed at other locations than at the company address of the data processor and at the location(s) specified in Sub-Appendix B (if applicable), without the data controller's prior written authorisation.

C.6. Instruction on the transfer of personal data to third countries
If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor
The data controller may audit/inspect the data processor's compliance with the Clauses on an annual basis.

To request an audit, the data controller must either provide a questionnaire to be filled out by the data processor or submit a detailed inspection plan at least three (3) months in advance of the proposed inspection date to the data processor, describing the proposed scope, duration, and start date of such inspection.

The data processor shall, on an annual basis, undergo an ISAE 3000 and ISAE 3402 audit report performed by an independent third-party auditor, unless otherwise determined at the discretion of the data processor. The data controller shall accept the findings of such audit reports, as well as any other audit reports conducted by an independent third-party auditor with the past twelve months, instead of requesting a new audit for the measures covered by the reports, provided that the data processor confirms there have been no known material changes to the audited measures.

Agreed upon physical inspections must be conducted during regular business hours at the applicable facility, subject to the data processor's policies, and may not unreasonably interfere with the data processor's business activities.

Based on the results of the audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller shall be responsible for all costs arising from the data controller's audits/inspections.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor carries out annual audits/inspections with its sub-processors in order to determine the sub-processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or Member States' national law and these Clauses.

Audits may take the form of written information gathering (questionnaire response) and inspections in the form of a physical inspection of the premises from which the sub-processor processes personal data, including systems used for or in connection with the processing.

The data processor bases its choice of either audits or inspections incl. the frequency on a risk assessment.

If the sub-processor(s) receives an annual audit report from an independent third party regarding the sub-processor's compliance with these Clauses and the technical and organisational security measures agreed herein, the data controller shall receive a copy thereof upon request. The data processor reviews the audit report and follows up on any issues that require further investigation.

The data processor documents all audits/inspections carried out, including any significant findings. At the request of the data controller, a short summary of the audit/inspection shall be sent without undue delay to the data controller.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to audits/inspections regarding the sub-processor's compliance with the General Data Protection Regulation and the Clauses shall not concern the data controller.

Sub-Appendix D (The parties' terms of agreement on other subjects)

1) THE DATA CONTROLLER'S INSTRUCTIONS (CHANGE TO CLAUSE 4.2)

Notwithstanding Clause 4.2., the data processor shall not be obliged to actively verify or investigate the legality of the data controller's instructions. To the extent that the data controller gives instructions to the data processor, which subsequently turns out to be illegal, the data controller is obliged to indemnify the data processor for any loss as a result including, without limitation, from any claim against the data processor arising therefrom, including claims from third parties, the affected data subjects and sub-processors.

2) CONFIDENTIALITY (ADDITION TO CLAUSE 5)

The data processor shall not disclose information related to the Clauses, including personal data, to governmental authorities, including the police, unless required by law, such as through a court order.

3) REQUESTS FROM THE DATA CONTROLLER

Any request from the data controller in regard to the data processor's compliance with the Clauses must be relevant in regard to the specific processing activities carried out by the data processor and the associated risk(s).

4) AMENDMENTS

These Clauses are subject to ongoing review, and any changes will be communicated to the data controller at least thirty (30) days prior to their effective date, except changes concerning the addition or replacement of sub-processors, in which case the data controller shall be notified of such changes in accordance with Clause 7.3.

5) SEVERABILITY

If any provisions in these Clauses become invalid, illegal, or unenforceable, then it shall not affect the validity of the remaining Clauses. The parties shall in such case, be entitled to request that a valid and practicable clause be negotiated which fulfils the purpose of the original clause and ensures that the Clauses fulfills the requirements under GDPR Article 28 in general.

6) LIABILITY

The Parties agree and acknowledge that each Party shall be liable for and held accountable to pay administrative fines and damages which the Party has been imposed to pay by the data protection authorities or authorized courts according to EU or Member State law. Liability matters between the Parties, including claims for indemnification of third-party claims, shall be governed by the liability clauses outlined in clause 14 of the General Terms and Conditions for Addo Sign.

7) ASSISTANCE

The data processor reserves the right to charge the data controller a reasonable fee for any assistance (cf. Clause 9), provided beyond what is considered reasonable under these Clauses. Such assistance may include, but is not limited to:

- Support required due to the data controller’s non-compliance with GDPR or other applicable data protection laws.
- Efforts necessitated by the data controller’s failure to provide necessary information or instructions in a timely manner.
- Assistance with excessive or repetitive data subject requests that exceed the ordinary course of business.
- Additional measures needed to address data breaches caused by the data controller's actions or omissions.

The fee for such assistance will be based on the data processor's hourly rates which is DKK 1063 excl. VAT.

8) GOVERNING LAW AND VENUE

The Clauses are governed by clause 18 of the General Terms and Conditions for Addo Sign, which pertains to governing law and venue.