DATA PROCESSING AGREEMENT (DPA)
Standard Contractual Clauses

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

between

the data controller

and

the data processor:
e-Boks Nordic A/S
CVR-NO 25674154
Hans Bekkevolds Allé 7
2900 Hellerup
Denmark

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. Table of Contents

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 the context of the provision of the general terms and conditions for sending customers for use of the e-Boks services (General Terms and Conditions) the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

5. Four (4) appendices are attached to the Clauses and form an integral part of the Clauses.

6. 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. 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. 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. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with 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[1] 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 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 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 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.

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

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 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 30 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 Appendix B. The list of sub-processors already authorised by the data controller can be found in 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 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 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 72 hours after having become aware of it, notify the personal data breach to the competent national supervisory authority in Denmark (The Danish Data Protection Agency), in Norway (The Norwegian Data Protection Authority) or in Sweden (The Swedish Data Protection Authority), 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 in Denmark (The Danish Data Protection Agency), in Norway (The Norwegian Data Protection Authority) or in Sweden (The Swedish Data Protection Authority) 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 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 48 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 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 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 appendix C.7.

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 at whichever time is earliest; when the data controller uses the data processor's services as defined in Appendix A, clause A.1, or when the data controller approves the data processor's terms and conditions for sending customers and/or these Clauses.

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 Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

1. The data processor may contact the data controller using the contacts/contact points given by the data controller when approving this DPA.

2. The data controller may contact the data processor´s legal/compliance department via e-mail (dpo-team@e-boks.dk) or telephone (+ 45 70 21 24 00).

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

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 data processor shall process personal data for the purpose of providing the e-Boks services to the data controller according to the data processor's General Terms and Conditions (collectively with the Clauses and any other agreement(s) between the parties these shall be referred to as "the Agreement" hereinafter), including without limitation providing a secure digital communication solution for communicating with end-users.

The data processor shall process personal data under the terms and conditions of this DPA in order to provide the services to the data controller according to a main agreement between the parties and/or the data processor's General Terms and Conditions, which may include providing the following:

- secure distribution of electronic mail
- secure reply to electronic mail
- digital signing of documents
- digital payment
- portal solutions for secure digital communication
- physical print output

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):

When the data controller submits messages/personal data for delivery in the end-user's digital mailbox (either directly or through a distributor or partner) the data processor is processing personal data on behalf of the data controller. This DPA applies to the data processors processing of personal data for the data controller.

When the messages/personal data is placed/delivered in the digital mailbox of an end-user, the data processor is then processing personal data on behalf of the end-user and not the data controller. This DPA does not apply to the data processor's processing of personal data for the end-user.

When physical messages/personal data is delivered to a third-party distribution supplier such as PostNord, the data processor is no longer processing personal data on behalf of the data controller.

A test environment is open to the data controller. However, it is not allowed to upload and/or utilize personal data in the test environment.

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

The data processor´s processing may include the following types/categories of ordinary personal data:

- Ordinary personal data (name, address, IP-address, phone number, e-mail address, shipmentID, message-ID, transaction-ID, transaction data, log data, meta data for receiving and sending messages, DPID-numbers, UUID-Numbers),
- free text (fritekst) in messages,
- information about criminal offences, and
- social security numbers.

The content of the messages that the data controller submits to the data processor for placement in the end-user's digital mailbox is decided by the data controller and thereby contains free text (fritekst) that may contain a wide range of personal data including special categories of personal data, including information concerning:

- Racial or ethnic background,
- political beliefs,
- religious beliefs,
- philosophical beliefs,
- union membership,
- health, including genetic and biometric data, and
- sexual orientation.

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

The processing of personal data includes personal data regarding data controllers, data controllers' employees, and end-users as defined by the data controller (or their customers as sending customers), including their customers, members, insurance policy holders, pensioners, employees, as well as their spouses, cohabitants, children, beneficiaries, employers, and others that receive and send electronic mail to and from the data controller, or other registered persons that may be mentioned in the content of the messages (the free text/fritekst).

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:

When the data controller submits messages/personal data for delivery to the end-user as agreed, the duration of the processing is determined by the data controller.

When physical messages/personal data is delivered to a third-party distribution supplier such as PostNord, the data processor's processing of personal data on behalf of the data controller ends.

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 OF COMPANY	ORG. NR	COMPANY ADDRESS	DESCRIPTION OF PROCESSING	REMARKS
e-BOKS SOLUTION				
KMD A/S	26911745	Lautrupparken 40 2750 Ballerup Denmark	Hosting the e-Boks solution.	Processing locations within the EU/EEA: - Denmark
Stratu ApS	42543039	Lautruphøj 5 - 7 2750 Ballerup Denmark	Hosting the e-Boks solution.	Processing locations within the EU/EEA: - Denmark
e-Boks Development A/S	42309745	Hans Bekkevolds Alle 7 2900 Hellerup Denmark	Operation and maintenance.	Processing locations within the EU/EEA: - Denmark
Kyndryl Denmark ApS (sub-processor to KMD A/S)	41988169	Prøvensvej 1 2605 Brøndby Denmark	Hosting the e-Boks solution.	Processing locations within the EU/EEA: - Denmark
Kyndryl Ireland Limited (sub-processor to KMD A/S)	66 86 75	Building 5 Damastown Industrial Estate Mulhuddart, Dublin 15 Ireland	Support services related to hosting.	Processing locations within the EU/EEA: - Ireland
Kyndryl Hungary Kft. (Kyndryl Hungary Korlátolt Felelősségű Társaság)	Cg. 07-09-031714	Gabor Denes Utca 2, Infopark D, Budapest, 1117 Hungary	IT operation services related to hosting.	Processing locations within the EU/EEA: - Hungary

NAME OF COMPANY	ORG. NR	COMPANY ADDRESS	DESCRIPTION OF PROCESSING	REMARKS
(sub-processor to KMD A/S)				
Aeven A/S (sub-processor to KMD A/S)	43432133	Østmarken 3A, 2860 Søborg, Denmark	Hosting the e-Boks solution.	Processing locations within the EU/EEA: - Denmark
Aeven Czech Republic s.r.o. (sub-processor to KMD A/S)	031 37 236	Explora Jupiter Bucharova 2641/14 3.NP, CZ-158 00, Prague, Czech Republic	IT operation and support services related to hosting.	Processing locations within the EU/EEA: - Czech Republic
Aeven Hungary Kft. (sub-processor to KMD A/S)	01-09-432639	Népfürdö utca 22 Building B 13th. Floor, 1138, Budapest, Hungary	IT operation and support services related to hosting.	Processing locations within the EU/EEA: - Hungary
Signing service Only applicable if the controller utilizes the signing service.				
Trust Services ApS	44526778	C/O Nets Denmark A/S Klausdalsbrovej 601 Denmark	Providing the optional signing Services.	Processing locations within the EU/EEA: - Denmark
Direct Only applicable if the controller utilizes the e-Boks Direct service.				
Parajett AB	5560068974	Box 63 261 22 Landskrona Sweden	Providing optional printing and enveloping services.	Processing locations within the EU/EEA: - Sweden

NAME OF COMPANY	ORG. NR	COMPANY ADDRESS	DESCRIPTION OF PROCESSING	REMARKS
Parajett Digital Solutions AB (sub-processor to Parajett AB)	5592815756	Box 63 261 22 Landskrona Sweden	Providing optional printing and enveloping services.	Processing locations within the EU/EEA: - Sweden
Cygate AB (sub-processor to Parajett AB)	5565498952	Box 4045 Honnörsgatan 2 352 36 Växjo Sweden	Hosting of optional printing and enveloping services.	Processing locations within the EU/EEA: - Sweden
GleSYS AB (sub-processor to Parajett AB)	5566479241	Kanslistvägen 12 311 22 Falkenberg Sweden	Hosting of optional printing and enveloping services.	Processing locations within the EU/EEA: - Sweden
SMS notification Only applicable if the controller utilizes the SMS notification feature.				
Sinch Denmark ApS	26361710	Fruebjergvej 3 2100 København Ø Denmark	Providing optional SMS notification services.	Processing locations within the EU/EEA: - Denmark
Sinch Sweden AB (sub-processor to Sinch Denmark ApS)	5567475495	Lindhagensgatan 112 11251 Stockholm Sweden	Providing optional SMS notification services.	Processing locations within the EU/EEA: - Sweden
Sinch Operator Software AB (sub-processor to Sinch Denmark ApS)	5563531333	Lindhagensgatan 112 11251 Stockholm Sweden	Providing customer support, project management, deployment, and managed services	Processing locations within the EU/EEA: - Sweden

NAME OF COMPANY	ORG. NR	COMPANY ADDRESS	DESCRIPTION OF PROCESSING	REMARKS
			related to optional SMS notification services.	
Sinch Poland S.P. Zoo (sub-processor to Sinch Denmark ApS)	0000643951	Prosta 51 00-838 Warszaw Poland	Providing customer support, project management, deployment, network monitoring, and managed services related to optional SMS notification services.	Processing locations within the EU/EEA: - Poland
Amazon Web Services GmbH (sub-processor to Sinch Denmark ApS)	HRB 114708	Eschborner Landstrasse 100 60489, Frankfurt am Main, Germany	Hosting of optional SMS notification services.	Processing locations within the EU/EEA: - Germany

Upon notification to the data controller the data processor may replace Appendix B with a reference to the list of sub-processors made available for the data controller online.

B.2. Prior notice for the authorisation of sub-processors

The data processor shall inform the data controller of any planned changes regarding additions to or replacement of a sub-processor and thereby give the data controller the opportunity to object to such changes.

Any objections to notified changes shall be made in writing by the data controller as soon as possible and no later than 30 days after receiving a notification from the data processor. The data controller can only object on reasonable and specific grounds.

If the data controller submits a reasonable and specific objection against the use of a sub-processor within the deadline stated, the data processor shall take such objection into account.

However, if the data processor decides not to accommodate the objection, or if the data processor is unable to do so within a reasonable period of time, both parties are entitled to terminate the part of the Agreement that covers the service which would have given the sub-processor access to the personal data.

The affected part of the Agreement may be terminated without liability with effect when the change relating to the sub-processor is due to take effect. The other parts of the Agreement shall continue to apply according to the provisions of the Agreement between the parties including the data processor's General Terms and Conditions.

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 when providing the agreed services according to the data processor's General Terms and Conditions includes:

- collection
- registration
- systematization
- storage
- deletion
- updating
- forwarding
- delivery

In addition, the personal data may be included in the general statistics of the use of the services.

C.2. Security of processing

1. Technical and organizational measures
The data processor has implemented the necessary and relevant precautionary security measures in accordance with the areas identified in the Information Security Standard ISO 27001:2013 (Annex A).

The data processor ensures the following necessary technical and organizational security measures are implemented and effective when processing data covered in the Agreement.

a. Technical measures and procedures to ensure access to personal data is restricted and controlled based on the principle of least privilege and limited to personnel with a work-related need. Technical security measures for secure identification, authentication, and authorization for people to gain access to the systems. Procedures include management-based approval of authorized access with regular follow-up to ensure that authorization is continually conditioned.

b. All access to personal data is logged. Technical measures register denied attempts to access personal data described in the Agreement. Logged information can help to clarify and possibly prevent unauthorized access and misusage of personal data. The registration includes denied attempts because of invalid identification, authentication, or authorization.

c. Technical measures for strong encryption of personal data in transition based on acknowledged algorithms and protocols.

d. Technical measures and procedures that hinder the risk of unauthorized execution of code and inhibits the installation of harmful software on it-systems used in the processing of personal data.

e. Incident response plans and procedures in case of system failure that ensures a timely recovery and accessibility of personal data.

f. Physical security measures to protect against unauthorized access and possible manipulation of personal data.

g. Procedures for regular testing, assessment, and evaluation of the effectiveness of technical and organizational security measures.

2. Organisation
The data processors´ security programme is anchored in the Security department, which is maintaining the Information Security Management System (ISMS). The ISMS is based on the ISO27001:2013 standard.

Besides a dedicated Security Department, security efforts are anchored in the security board and coordinated in cross functional groups.

The Security Board is the governing body for the overall security level and consists of C-level- and relevant area managers. The board convenes at regular intervals for risk handling and treatment but can also be assembled if the nature of a situation warrants an out-of-band meeting.

3. Responsibility
Onboarding employees includes confirmation of unblemished criminal record, signing of non-disclosure agreement, introduction to security policies and code of conduct. Awareness is sustained via the data processors awareness programme which is using a variety of channels and means to address information security and data privacy.

All employees must comply with the security policies and are obligated to actively prevent acts that may compromise the information security or information entrusted to the data processor.

The operational responsibility for the company's information security is delegated to the organization's administrative management, to correctly implement and administer the requirements of the ISMS in the form of Policies, Standards and Procedures.

Managers are responsible for overseeing employees' adherence to policies, standards, and procedures for Information Security. The responsibility includes the continual education of employees to maintain knowledge and competencies for handling their daily tasks in compliance with the policies, standards, and procedures. Violation of policies

and supporting regulations and procedures may lead to the sanctioning of an employee.

Upon termination of employment, the employee user accounts, and physical access are promptly terminated, and the employee is reminded of their obligation of non-disclosure.

4. Information Security and Data Privacy Policy
The ISMS consist of several general and area specific policies, all deriving from the overarching 'Information Security and Data Privacy Policy' which is anchored with the CEO and establishes high-level requirements and principles applicable to all solutions, staff, and suppliers. The policy emphasizes security and privacy as an invariable component of operations, considerations, and solutions.

The data processor must ensure documentation, which is required for the preservation of the information security and data privacy of the organization, is controlled, protected and available for employees and relevant stakeholders. This includes Policies, Standards, and Procedures, which establish security related requirements, instructions and specify implementation practices.

5. Security
The data processors solution is secured through multiple levels of security, including but not limited to:

5.a. Zones, Segregation and Firewalls
e-Boks infrastructure is segregated into multiple network zones, each adding extra level of protection. Traffic and access through zones are limited by IP-protection, firewalls, and certificates.

5.b. Availability and monitoring
Services are delivered out of several data centres to remediate a single points of failure. The data centres are located on different physical locations and protected with redundant connectivity, cooling humidity, fire detection and suppression, redundant power connections and backup power generators.

The premises are also protected by strong physical security measures, including CCTV, electronic access control systems and alarm systems with duty guards. Access to premises follows similar access control processes as system access.

All services are monitored, and plans are in place to respond to unplanned interruptions to e-Boks availability.

Data is backed up at regular intervals, backups are stored safely and verified to ensure data restoration is possible.

5.c. Workstation Security

Computers in e-Boks are subject to timely patching and operational policies including but not limited to, Automatic screen lock, Full disk encryption, Firewall, advanced malware protection and continual endpoint hardening.

5.d. Access Control and Event Logging

End-user access
Access for customers and end-users in the platform is exclusively provided using a national identity authentication standard. Log-on attempts, events and activities are logged.

Back-end access
The data processor has strict access control policies – both technical and administrative – and employ tight controls for access to production services and data, such as least principle, unique identifiers, password policies, multi-factor approval. Additionally, access rights and users are reviewed and attested at regular intervals and segregation of duties are enforced.

Acts of systems access is registered and all access and events in production environment are logged and stored in a central log repository.

System integrations
The data processor receives documents from senders using several interfaces which are protected with certificate-based access to ensure the authenticity of the sending organisation and encryption in transit. For interfaces without certificate-based access, there are compensating controls to ensure the validity of the senders and segment the input from the core of the solution as well as encryption in transit.

5.e. Spoof prevention
To prevent spoofing and phishing attacks pretending to be from the data processor, all e-mail enabled data processor domains are protected using anti spoofing technology in the form of DMARC which is configured as strict as possible.

5.f. Encryption and Protection of Data in Transit
All data is encrypted in transit between sender, platform, and user. Additionally, selected data is encrypted between security zones within the platform. The data processor follows recommendations from ENISA and PCI-DSS for encryptions standards, cipher suites and key lengths.

5.g. Equipment Decommission
Data carrying media used for information classified as Confidential, are subject to thorough wiping before final decommission. Printed materials are subject to cross shredding.

5.h. Change and Release management

All changes to Production environments are controlled according to the change and release processes, ensuring quality control, accountability, origin of change and version control.

5.i. Operational Security
Servers are protected using, privileged identity management technologies, firewalls, advanced malware protection, review of installed software and continued hardening. Vulnerability scanning is performed regularly and supported through established processes and standards. Servers are patched at scheduled intervals closely aligned with software vendors planned release of updates. Redundant architecture ensures availability during patching operations. Out of band patches are reviewed on a case-by-case basis for applicability and risk profile.

6. Contingency Planning and Crisis Management
If an incident cannot be contained to the parameters of the incident management process, it can be escalated to 'Disaster' status. The Crisis management plan holds greater mandate to make sure all necessary resources are made available for the treatment of a disaster.

6.a. Disaster Recovery Test
At least once annually the data processor performs a disaster recovery test of the technical resilience, such as testing the failover mechanisms of redundant technologies, data centres or test that the services provided performs as expected in adverse situations. Scope of testing is defined based on risk profile and major changes.

6.b. Crisis Management
e-Boks performs annual exercises to ensure the data processors ability to respond to adverse situations and ensure technological recovery are performed in a controlled manner as well as ensure stakeholders are informed at an adequate level.

Outcome of contingency tests are reported to the Security Board and observations that need attention are registered and tracked in the respective treatment processes.

7. Compliance
The data processor may use the following types of auditor's report as documentation of compliance to applicable security policies and measures:

- ISAE 3000 Type II Data processing Agreement
- ISAE 3000 type II General IT controls
- ISAE 3000 Type I ISO 27001 compliance

Outcome of compliance activities are reported to the Security Board and observations that need attention are registered and tracked in the respective treatment processes.

The data processor must, at the request of the data controller, once a year provide auditor reports of assurance, which cover the period from the latest audit.

C.3. Assistance to the data controller

The data processor shall assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the technical and organisational measures mentioned in C.2.

C.4. Storage period

The personal data is stored until placement of the messages in the end-user's digital mailbox. When the messages/personal data is placed/delivered in the digital mailbox of the end-user, the data processor`s processing of personal data on behalf of the data controller ends.

The personal data shall not be stored by the data processor longer than necessary for the purposes for which it was processed according to the data processor's retention standard.

C.5. Processing location

Processing of the personal data under the Clauses will be performed by the data processor at the data processor's location in EU/EØS. Processing by the authorised sub processors can be performed at other locations as mentioned in Appendix B1.

C.6. Instruction on the transfer of personal data to third countries

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in GDPR Chapter 5 are met.

The data processor shall inform the data controller of any planned changes regarding transfer of personal data to third countries and thereby give the opportunity to object to such changes.

Any objections to notified changes shall be made by the data controller as soon as possible and no later than 30 days after receiving a notification from the data processor.

The data controller can only object on reasonable and specific grounds.

If the data controller submits a reasonable and specific objection within the deadline stated, the data processor shall take such objection into account.

However, if the data processor decides not to accommodate the objection or if the data processor is unable to do so within a reasonable period of time, both parties are entitled to terminate the part of the Agreement that covers the service which would have been affected by the transfer.

The affected part of the Agreement may be terminated without liability, effective from when the change relating to the transfer is due to take effect. The other parts of the Agreement shall continue to apply according to the provisions of the Agreement between the parties including the General Terms and Conditions.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

To the extent that the data controller requests an audit, the data processor will make the processing systems and facilities accessible to the data controller according to the data processor`s audit policy in force at any given time. The audit policy is available by request.

Appendix D The parties' terms of agreement on other subjects

D.1. Expenses, costs, and fees.
The data processor, taking into account the nature of the processing, shall, as far as possible, assist the data controller.

The data processor shall make available to the data controller the reasonable information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this DPA. However, if the data controller requires information and/or documentation which is beyond the data processor´s own internal and standard documentation the data controller shall cover all expenses for the data controller to provide the necessary information/documentation.

The data controller shall bear all costs and fees related to an audit, including all reasonable costs and fees for the data processor´s expenses for an audit.

When assisting the data controller in a personal data breach the data processor shall provide the assistance at the data controller´s expense unless such personal data breach is due to circumstances attributable to the data processor or the data processor´s sub-processor.

D.2. Liability
The data processor's liability and limitation of liability is governed by the data processor's General Terms and Conditions.

D.3 Alterations and amendments
The data processor shall be entitled to alter and amend these Clauses at any time. Material changes shall only apply 6 months after notification to the data controller. The parties agree that any such alterations and amendments shall be made available on the following URL.

D.4. Greenland
If the processing involves transfer of personal data to Greenland, the data controller accepts that the standard contractual clauses contained in Sub-Appendix D.1 as published on the following URL at any given time shall be contained in these Clauses and enter into force on the same terms as these Clauses.