Data Processing Agreement

Data Processing Agreement
Version 6, 8.10.2026 13:07

FDE A/S ("the Organization")
Lyren 1, Bovmark
6330 Padborg
DK
CVR: 15452986

Table of Contents

1. Parties
2. Preamble
3. The rights and obligations of the Controller
4. The Processor acts according to instructions
5. Confidentiality
6. Security of processing
7. Use of sub-processors
8. Transfer of data to third countries or international organisations
9. Assistance to The Controller
10. Notification of personal data breach
11. Erasure and return of data
12. Audit and inspection
13. The parties' agreement on other terms
14. Commencement and termination
15. The controller and the processor contacts/contact points
16. Appendix A - Information about the processing
17. Appendix B - Sub-processors
18. Appendix C - Instruction pertaining to the use of personal data
19. Appendix D - The parties' regulation of other matters
20. Appendix E - Standard Contractual Clauses for the transfer of personal data to third count

1. Parties

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

between

The customer, hereinafter "The Controller"

and

FDE A/S
Lyren 1, Bovmark
6330 Padborg
DK
Company registration number: 15452986

hereinafter "The 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.

2. Preamble

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

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 (GDPR).

In the context of the provision of Applicable commercial agreement(s), the Processor will process personal data on behalf of the Controller in accordance with the Clauses.

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

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

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.

Appendix B contains the Controller's conditions for the Processor's use of sub-processors and a list of sub-processors authorised by the Controller.

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

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

If standard contractual clauses as referred to in GDPR, Article 46(2), litra c and d form basis of transfer of personal data between the Controller and the Processor covered by chapter V of the GDPR, these will be attached as Appendices E and E1.

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

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

3. The rights and obligations of the Controller

The 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.

3.1 The Data Controller's decision-making authority

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

3.2 Basis for processing personal data

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

4. The Processor acts according to instructions

The Processor shall process personal data only on documented instructions from the 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 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.

4.1 Notification of infringing instructions

The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1 Access to personal data and confidentiality

The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the 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.

5.2 Documentation of obligation of confidentiality

The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1 Technical and organisational measures

GDPR, Article 32, 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 Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The 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:

1. Pseudonymisation and encryption of personal data;
2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 Risk assessment of the Processor

According to GDPR, Article 32, the Processor shall also – independently from the 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 Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

6.3 Assistance with compliance with security measures

Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR, Article 32, by inter alia providing the Controller with information concerning the technical and organisational

measures already implemented by the Processor pursuant to GDPR, Article 32, along with all other information necessary for the Controller to comply with the Controller's obligation under GDPR, Article 32.

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

7. Use of sub-processors

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

7.1 General written authorisation

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

The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 in advance, thereby giving the 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 Controller can be found in Appendix B.

7.2 Sub-processor obligations

Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the 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 GDPR.

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

7.3 Documentation of sub-processor agreements

A copy of such a sub-processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the 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 Controller.

7.4 Third party benificiary clause

The Processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.5 Liability for sub-processors

If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the 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 GDPR, Articles 79 and 82 – against the Controller and the Processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 Instructions on transfers to third countries

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

Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Clauses:

1. transfer personal data to a controller or a processor in a third country or in an international organization
2. transfer the processing of personal data to a sub-processor in a third country
3. have the personal data processed by the Processor in a third country

The 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.

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

8.2 Notification of legally required transfers

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

9. Assistance to The Controller

9.1 Assistance with data subject rights request

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

This entails that the Processor shall, insofar as this is possible, assist the Data Controller in the Controller's compliance with:

1. the right to be informed when collecting personal data from the data subject
2. the right to be informed when personal data have not been obtained from the data subject
3. the right of access by the data subject

4. the right to rectification
5. the right to erasure ('the right to be forgotten')
6. the right to restriction of processing
7. notification obligation regarding rectification or erasure of personal data or restriction of processing
8. the right to data portability
9. the right to object
10. the right not to be subject to a decision based solely on automated processing, including profiling

9.2 Assistance with data breaches and data protection impact assessments

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

1. The 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 data protection agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
2. The 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;
3. The 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);
4. The Controller's obligation to consult the competent 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 Controller to mitigate the risk.

9.3 Specification of Technical and Organisational Assistance Measures in Appendix C

The Parties shall define in Appendix C the appropriate technical and organisational measures by which The Processor is required to assist the controller as well as the scope and the extent of the assistance required. This applies to the obligations forseen in Clause 9.1 and 9.2.

10. Notification of personal data breach

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

10.1 Notification deadline for Personal Data Breaches

The Processor's notification to the Controller shall, if possible, take place within and by the latest 24 hours after the Processor has become aware of the personal data breach to enable the Controller to comply with the Controller's obligation to notify the personal data breach to the data protection agency, cf. GDPR, Article 33.

10.2 Assistance with notification of breaches

In accordance with Clause 9.2.1, the Processor shall assist The Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to GDPR, Article 33(3), shall be stated in the Controller's notification to the competent data protection authority:

1. 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;
2. the likely consequences of the personal data breach;
3. 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.

The parties shall define in Appendix D all the elements to be provided by the Processor when assisting the Controller in the notification of a personal data breach to the competent data protection agency.

11. Erasure and return of data

11.1 Erasure of personal data on termination

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

11.2 Storage on the basis of legal obligation

The following EU or Member State law applicable to the Processor requires storage of the personal data after the termination of the provision of personal data processing services:

1. Deletion is subject to accounting rules unless otherwise stated in the customer agreement.

The Processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. Audit and inspection

12.1 Assistance with audits and inspections

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

12.2 Procedures for audits and inspections

Procedures applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in C.7 .

12.3 Access for supervisory authorities

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

13. The parties' agreement on other terms

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

14.1 Effective date

The Clauses are binding upon the Parties.

14.2 Renegotiation

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.

14.3 Duration

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.

14.4 Termination

If the provision of personal data processing services is terminated, and the personal data is deleted to the Controller pursuant to Clause 11.1 and Appendix C.4, the Clauses may be terminated by written notice by either Party.

14.5 Binding Effect

The Processor is bound by the Clauses without the Parties' signatures. The Clauses are thus entered into without physical/ digital signatures, as the Clauses are binding in accordance with the requirement set out in GDPR, Article 28(3).

15. The controller and the processor contacts/contact points

The Parties may contact each other using the following contacts/contact points. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for The Controller:

The contact information for the Data Controller is provided in the Main Agreement.

Contact information for The Processor:

The contact information for the Data Processor is provided in the Main Agreement.

16. Appendix A - Information about the processing

16.1 The purpose of the Processor’s processing of personal data on behalf of the Controller

The following purposes form the basis of the Processor's processing of personal data on behalf of the Controller:

The Personal Data is processed with the sole purpose of providing the commercial services covered by the commercial agreement(s) to which this DPA is an appendix

16.2 The Processor’s processing of personal data on behalf of the Controller shall mainly pertain to (the nature of the processing):

The Personal Data is processed with the sole purpose of providing the commercial services covered by the commercial agreement(s) to which this DPA is an appendix.

16.3 Types of personal data

The processing includes the following types of personal data concerning the data subjects:

- Address
- Bank details (card details or account information)
- Username for one or several systems
- Social security number
- E-mail
- Billing and accounting records
- Date of birth
- Name
- Information about users' used device
- Phone number
- Various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof

16.4 Categories of data subjects

The processing includes the following categories of data subjects:

- Affiliates that are individuals or sole proprietorships
- Current employees
- Customers that are consumers or sole proprietors
- Customers' customers and their employees (for example to CRM suppliers)
- Customers' employees (when customers are companies)
- Suppliers that are persons or sole proprietors
- Suppliers' employees (when the suppliers are companies)

16.5 Duration

The Processor’s processing of personal data on behalf of the Controller may be performed when the Clauses commence.

The processing of personal data shall be performed until the Processor's services has been terminated, after which the personal data is erased in accordance with Clause 11. The Processor's processing of personal data is performed as long as the underlying commercial agreement(s) consists.

17. Appendix B - Sub-processors

17.1 Approved sub-processors

On commencement of the Clauses, the Controller authorises the engagement of the following sub-processors:

ITD Holding A/S, Lyren 1, 6330 Padborg. ITD Holding operates and delivers all IT to the Data Processer and processes personal data in this connection.
Local agents and VAT handlers. These third parties are specified to and accepted by each customer in connection with collection and signature of power of attorney from the relevant customer to the relevant agent or VAT handler. The Data Controller acknowledges that - irrespective of other terms in this Data Processor Agreement - such acceptance and signature of a power of attorney shall constitute acceptance of the same third party as a sub-data processor.

18. Appendix C - Instruction pertaining to the use of personal data

18.1 The subject of/instruction for the processing

The Personal Data is processed with the sole purpose of providing the commercial services covered by the commercial agreement(s) to which this DPA is an appendix.

18.2 Security of processing

The level of security shall take into account:

Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Processor must implement an appropriate level of security.

The Processor shall hereafter 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) level of data security.

The Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Controller:

Physical security
The Processor shall implement the following physical security measures:

- A protocol is kept of the Processor's visitors.
- Reception is staffed 24/7 or there is a security company outside of office hours.
- The Processor has tested the contingency and evacuation plan for emergencies.
- The Processor uses a verification process or verification system to control the identity of visitors.
- The Processor uses alarm systems to detect and prevent burglary.
- The Processor uses fire alarms and smoke detectors to detect and prevent fires.
- The Processor uses key management, i.e. provide keys to the relevant and necessary employees, etc.
- The Processor's building(s) are divided into access zones, after which access cards are required for access to the zones.
- The Processor's devices (including PCs, servers, etc.) are secured behind locked doors.
- The Processor's office space can be locked.

Organisational security measures
The Processor shall implement the following organisational security measures:

- All employees of the Processor are subject to confidentiality obligations that apply to all processing of personal data
- The employee access to personal data is limited, so that only the relevant employees have access to the necessary personal data
- The processing of personal data done by the employees of the Processor is logged and can be checked as required
- The Processor has an IT security policy
- The Processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually
- The Processor has established procedures that ensure proper deletion or continuous confidentiality when the hardware is repaired, serviced, or disposed
- The Processor has the opportunity to respond to employees' breaches of the processor's data security or breach of instructions on the processing of personal data according to employment law
- The Processor's employees regularly document and report breaches of personal data security or risks thereof

Technical security: Access to and protection of IT systems
The Processor shall implement the following technical security measures regarding access to and protection of IT systems:

- The Processor has policies for password composition, including minimum requirements
- The Processor requires employees to use individual passwords
- The Processor uses antivirus programs that are updated regularly
- The Processor uses logical access control with username and password or other unique authorization
- The Processor's computers have automatic access protection during inactivity, ie. locked screen saver
- There are procedures for granting authorizations to IT systems when hiring new employees
- There are procedures for revoking permissions when an employee stops or switches department

Technical security: Access to personal data
The Processor shall implement the following technical security measures regarding access to personal data:

- The Processor grants authorizations to individuals or groups of users to access, change and delete processed personal data
- The Processor has procedure(s) to restore data from backup
- The Processor has traceability of access, modification and erasure of data by individual users
- The Processor regularly reviews and verifies user authorizations for specific systems
- The Processor regularly reviews system controls

Technical security: Encryption
The Processor shall implement the following technical security measures regarding encryption:

- The network is encrypted
- The Processor's websites and web forms uses SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure)

Technical security: Protection of personal data during transmission
The Processor shall implement the following technical security measures regarding protection of personal data during transmission:

- Outgoing emails with sensitive personal data or information about purely private matters are encrypted
- The Processor has guidelines for the use of work emails, including use for private use, appropriate use, encryption, secure use, etc
- The Processor uses and has guidelines for secure email

Technical security: Availability and robustness
The Processor shall implement the following technical security measures regarding availability and robustness:

- Active alerting by unauthorized attempts to access server rooms and/or processing systems and data
- Backups are made regularly (either in-house or at supplier)
- Monitoring of temperature and humidity in server rooms
- Only authorized employees have access to the Processor's own servers
- Server room has air conditioning system
- Server rooms have smoke alarms and fire extinguishers
- There are rules and guidelines for data backup
- There are rules and guidelines for restoring data from backup
- The processor has procedure descriptions for breaches of the personal data security that are reviewed at least annually
- Uninterruptible power supply (UPS) is used

18.3 Assistance to the Controller

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

- If the Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Processor, the Processor shall assist the Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.
- If the Controller needs the Processor's assistance in order to reply to a request from a data subject, the Controller must send a written requst for assistance to the Processor and the Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after receiving the request.
- If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the reuest to The Controller.

18.4 Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the Processor shall delete the personal data in accordance with Clause 11.1 unless the Controller – after the signature of the contract – has modified the Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

18.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Controller's prior written authorisation:

At the Processor's own headquarter or at the headquarters of approved subprocessors as specified in Appendix B.

18.6 Instruction on the transfer of personal data to third countries

Personal data is only being processed by the Processor on the locations specified in this appendix.

Transfers to the United States occur on the basis of the data importer's certification under the EU-U.S. Data Privacy Framework (see certified organisations here.)

Safe third countries
As part of complying with the Clauses, the Data Processor transfers the personal data to the following countries:

- Faroe Islands
- Switzerland
- United Kingdom

Such transfers are based on decisions of the European Commission, which generally ensure a sufficient level of protection, either through legislation or through other measures.

Unsafe third countries
The Data Processor transfers personal data to the following countries not subject to an adequacy decision on the basis of Article 45 of Regulation (EU) 2016/679t in order to fulfill the Main Agreement: USA

When in relation to these Clauses, Personal Data is transferred to third countries outside the EU / EEA, not subject to an adaquacy decison on the basis of GDPR, Article 45, the legal basis shall be standard contractual clauses pursuant to GDPR, Article 46(1) and Article 46(2)(c). If the Controller is functioning as a processor, under the instruction of a third party controller, and the Processor acts as a sub-processor, in this respect, the legal basis shall likewise be standard contractual clauses.

Insofar as personal data, for which both parties are data controllers, is transferred between, to a third country outside the EU / EEA, not subject to an adaquacy decison on the basis of GDPR, Article 45, and this transfer in not subject to one or more of the exemption rules in GDPR, Article 49, the legal basis shall likewise be standard contractual clauses as contained in Appendix E.

General
If the Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Processor is not entitled to carry out such transfers within the scope of these Clauses.

Transfer of personal data can in all cases only be done in accordance with these Clauses, on the instructions of The Controller and to the extent permitted by the applicable data protection law.

Where, in accordance with these clauses, The Processor transfers personal data to subdata processors in third countries outside the EU / EEA, the Processor must independently secure a legal basis for the transfer in accordance with Chapter 5 of GDPR.

18.7 Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor

The Processor shall, upon the Controller's written request, document to the Controller that the Processor

- is complying with his obligations under these Clauses and the Instruction, and
- with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Controller.

The Processor's documentation shall be sent to the Controller within a reasonable time after receiving the request.

The processor must provide the controller with documentation of continuous compliance with the provisions. These self-audit reports must be prepared at least once a year and shall follow the principles and control objectives of the ISAE 3000 auditing standard, as laid down by FSR - Danish Auditors and the Danish Data Protection Agency (and/or alternatively internationally recognized standards such as ISO/IEC 27701:2019). Self-audit reports may be conducted as part of the controller's information gathering and must be signed by the processor's management.

The Processor shall furthermore provide for and contribute to audits and inspections every 12 months, performed by auditors appointed by the Controller, the public authorities in the competent jurisdiction, to the extent necessary to verify the Processor's compliance with these Clauses and the applicable data protection law. The auditor in question must be subject to confidentiality under law or agreement. The Controller must notify the audits in writing with 7 calendar days .

19. Appendix D - The parties' regulation of other matters

19.1 Other matters

The Data Processing Agreement does not govern other matters.

20. Appendix E - Standard Contractual Clauses for the transfer of personal data to third count

Regarding transfer of personal data to the Data Processor in a third country that does not ensure adequate level of data protection, and according to GDPR, article 46, the Parties have agreed to the following Standard Contract Clauses in order to provide appropriate safeguards regarding the protection of privacy and the fundamental rights and freedoms of natural persons in relation to the disclosure of personal data by the data exporter in this Agreement, including Appendix A, B, C and D.

Unless otherwise provided in this Appendix E, words and phrases with a capital letter have the same meaning as set out in the Agreement, including Appendix A, Appendix B, Appendix C and Appendix D.

The Standard Contractual Clauses regulate all transfers between the Parties, conducted in connection with the services governed by the Data Processing Agreement, to third countries outside the EU/EEA, not subject to an adaquacy decison on the basis of GDPR, article 45, insofar as none of the derogations for a specific situation referred to in GDPR, article 49 apply.

The appropriate modules take effect accordingly:

- **Module One** applies to transfers of personal data between the Parties for which both Parties are controllers, whether jointly or independently.

- **Module Two** applies to transfers of personal data from the Data Controller to the Data Processor, where the Data Controller is not acting as a processor for another ultimate data controller.
- **Module Three** applies to transfers of personal data from the Data Controller to the Data Processor, where the Data Controller is acting as a data processor on behalf of another ultimate data controller.
- **Module Four** applies to transfers of personal data from the Data Processor to the Data Controller, where the Data Controller is based in a third country outside the EU / EEA, not subject to an adaquacy decison on the basis of GDPR, article 45.

21. Section I

21.1 Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b. The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

21.2 Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to GDPR, article 46(1) and 46(2)(c), with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to GDPR, article 28(7), provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of GDPR.

21.3 Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii. Clause 8 – Module One: Clause 8.5.5 and Clause 8.9.2; Module Two: Clause 8.1.2, 8.9.1, 8.9.3, 8.9.4 and 8.9.5; Module Three: Clause 8.1.1, 8.1.3 and 8.1.4 and Clause 8.9.1, 8.9.3, 8.9.4, 8.9.5, 8.9.6 and

8.9.7; Module Four: Clause 8.1.2 and Clause 8.3.2;

iii. Clause 9 – Module Two: Clause 9.1, 9.3, 9.4 and 9.5; Module Three: Clause 9.1, 9.3, 9.4 and 9.5;

iv. Clause 12 – Module One: Clause 12.1 and 12.4; Modules Two and Three: Clause 12.1, 12.4 and 12.6;

v. Clause 13;

vi. Clause 15.1.3, 15.1.4 and 15.1.5;

vii. Clause 16.5;

viii. Clause 18 – Modules One, Two and Three: Clause 18.1 and 18.2; Module Four: Clause 18.

b. Paragraph 3.1 is without prejudice to rights of data subjects under GDPR.

• 21.4 Interpretation

a. Where these Clauses use terms that are defined in GDPR, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of GDPR.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in GDPR.

• 21.5 Hierarchy

a. In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

b. Paragraf 5.1 not withstanding, insofar as the contradiction with a later agreement between the parties strictly concerns the optional content of paragraf 9.1, and/or the Appendix, the later agreement shall prevail, provided this does not interfere with the function of the Clauses as sufficient safeguards pursuant to GDPR, article 46(1) and article 46(2)(c).

• 21.6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

• 21.7 Docking Clause (NOT IN EFFECT)

a. ~~An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.~~

b. ~~Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.~~

c. ~~The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.~~

22. Section II - OBLIGATIONS OF THE PARTIES

22.1 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE THREE: Transfer processor to processor (IN EFFECT)

1. **Instructions**
    a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
    b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
    c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
    d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].
2. **Purpose limitation**
    The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.
3. **Transparency**
    a. On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
    b. Insofar as the content matter of these Clauses and the Appendix is determined by reference to other agreements betweeen the parties, the relevant parts of such other agreements are likewise subject to the provisons of transparency contained in paragraph 8.3.1.
4. **Accuracy**
    If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.
5. **Duration of processing and erasure or return of data**
    Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause

14.5 to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14.1.

6. **Security of processing**

   a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

   b. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

   c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

   d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under GDPR, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

7. **Sensitive data**

   Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8. **Onward transfers**

   The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

   (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to GDPR, article 45, that covers the onward transfer;

   (ii) the third party otherwise ensures appropriate safeguards pursuant to GDPR, articles 46, or 47 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation

9. **Documentation and compliance**
    a. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
    b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
    c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
    d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
    e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
    f. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
    g. The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.

• 22.2 Data subject rights

MODULE THREE: Transfer processor to processor (IN EFFECT)

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under GDPR or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

• 22.3 Redress

MODULE THREE: Transfer processor to processor (IN EFFECT)

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.
4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in GDPR, article 80(1).
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

• 22.4 Liability

MODULE THREE: Transfer processor to processor (IN EFFECT)

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c. Notwithstanding paragraph 12.2, the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under GDPR or Regulation (EU) 2018/1725, as applicable.
d. The Parties agree that if the data exporter is held liable under paragraph 12.3 for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph 12.5, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

• 22.5 Supervision

MODULE THREE: Transfer processor to processor (IN EFFECT)

b. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

    [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with its article 3(2) and has appointed a representative pursuant to GDPR,

article 27(1):] The supervisory authority of the Member State in which the representative within the meaning of GDPR, article 27(1), is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with its article 3(2) without however having to appoint a representative pursuant to GDPR, article 27(2):] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

c. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

23. Section III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

• 23.1 Local laws and practices affecting compliance with the Clauses

MODULE THREE: Transfer processor to processor (IN EFFECT)

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in GDPR, article 23(1), are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph 14.1, they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [12];

   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph 14.2, it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph 14.1, including following a change in the laws of the third country or a

measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph 14.1. [For Module Three: The data exporter shall forward the notification to the controller.]

f. Following a notification pursuant to paragraph 14.5, or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16.4 and 16.5 shall apply

• 23.2 Obligations of the data importer in case of access by public authorities

MODULE THREE: Transfer processor to processor (IN EFFECT)

1. **Notification**

    a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

        i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

        ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. [For Module Three: The data exporter shall forward the notification to the controller.]

    b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

    c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the notification to the controller.]

    d. The data importer agrees to preserve the information pursuant to paragraphs 15.1.1 to 15.1.3 for the duration of the contract and make it available to the competent supervisory authority on request.

    e. Paragraphs 15.1.1 to 15.1.3 are without prejudice to the obligation of the data importer pursuant to Clause 14.5 and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

2. **Review of legality and data minimisation**

    a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if,

after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14.5.

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

24. SECTION IV – FINAL PROVISIONS

• 24.1 Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14.6.

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph 16.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph 16.3 shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph 16.3 shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to GDPR, article 45(3) that covers the transfer of personal data to which these Clauses apply;

or (ii) GDPR becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under GDPR

• 24.2 Governing law

MODULE THREE: Transfer processor to processor (IN EFFECT)

a. These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

• 24.3 Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor (IN EFFECT)

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of Denmark.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

Notes:

[1] Where the data exporter is a processor subject to GDPR acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to GDPR also ensures compliance with article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of the GDPR, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including GDPR, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including GDPR, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] See GDPR, article 28(4) and, where the controller is an EU institution or body, article 29(4) of Regulation (EU) 2018/1725.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including GDPR, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of

uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

25. Appendix E1

Annexes to Standard Contractual Clauses for the transfer of personal data to third countries

EXPLANATORY NOTE: Where information is available in the data processing agreement and associated appendices, references will be made. Followingly, parts of the dataprocessing agreement and appendices, or summaries thereof, may be required to be disclosed to the data subjects on request, pursuant to the provisoions of transparency contained in these Standard Contractual Clauses.

26. *ANNEX I*

A. LIST OF PARTIES

A.1 Data exporter:
Name:
FDE A/S
Address:
Lyren 1, Bovmark, 6330 Padborg, DK
Contact person's name, position and contact details:
The contact information for the Data Processor is provided in the Main Agreement.

Role (controller/processor):
Processor

Activities relevant to the data transferred under these Clauses:
Reference is made to the Data Processing Agreement.

Signature and date:
Reference is made to the Data Processing Agreement to which these Clauses form an appendix.

A.2 Data importer:
Name:
Microsoft Ireland Operations Limited
Address:
One Microsoft Place, South County Business Park, Leopardstown,
Dublin 18 D18 P521

Role (controller/processor):
Processor

Activities relevant to the data transferred under these Clauses:
Reference is made to the Data Processing Agreement.

Signature and date:
Reference is made to the data processing agreement to which these Clauses form an appendix.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:
Reference is made to Appendix A, paragraph 15.4 of the data processing agreement.

Categories of personal data transferred:
Reference is made to Appendix A, paragraph 15.3 of the data processing agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

No sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

The transfer(s) from controller to controller under these clauses will be of a continuous nature.

Nature of the processing:
Reference is made to Appendix A, paragraph 15.2 of the data processing agreement.

Purpose(s) of the data transfer and further processing:
Reference is made to Appendix A, paragraph 15.1 of the data processing agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
Reference is made to Appendix C, paragraph 18.4 of the data processing agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
Reference is made to Appendix B of the data processing agreement.

Subject matter
Reference is made to Appendix B of the data processing agreement.

Nature of processing
Reference is made to Appendix B of the data processing agreement.

Duration of processing
Reference is made to the data processing agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
Reference is made to the data processing agreement.

27. *ANNEX II*

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organisational measures taken by the Data Processor:
Reference is made to Appendix C, Clause 2 of the data processing agreement.

Technical and organisational measures taken by sub-processors:
Persuant to section 6 of the Data Processing Agreement, sub-processors must supply equivalent technical and organisational protective meassures, equivalent to those undertaken by the data processor.