Data Processing Agreement

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

between

Dstny customers
-
- -
DK
Company registration number: -
hereinafter "The Controller"

and

Dstny A/S (and group-affiliated companies)
Skodsborgvej 305 D
2850 Nærum
DK
Company registration number: 28313160
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.

This is version 2, last updated 29.09.2023 11:49.

1. **Content**

2. **Preamble**

2.1 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.

2.2 The parties are aware that the Controller is themself processing some or all of the personal data governed by the Clauses on behalf of another ultimate controller. In regard to this ultimate controller the Controller and Processor, thus function as processor and sub-processor respectively. The parties do not consider this fact to affect their obligations interpartes.

2.3 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).

2.4 In the context of the provision of mobile telephony, IP telephony, communication services and software (PBX, collaboration etc.), network infrastructure, security and related services, the Processor will process personal data on behalf of the Controller in accordance with the Clauses.

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

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

2.7 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.

2.8 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.

2.9 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.

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

2.11 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.

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

2.13 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.

2.14 Insofar as the Controller is in fact processing the relevant personal data on behalf of another ultimate data controller, this agreement shall function as a sub-processor agreement, in which case, Controller and Processor, shall be taken to mean processor and sub-processor respectively.

3. The rights and obligations of the Controller

3.1 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.

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

3.3 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

4.1 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.

4.2 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 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 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 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:

6.1.1 Pseudonymisation and encryption of personal data;

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

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

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

6.2 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 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

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

7.2 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.

7.3 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 days 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.

7.4 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.

7.5 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.

7.6 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 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.

8.2 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.

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

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

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

8.3.3 have the personal data processed by the Processor in a third country

8.4 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.

8.5 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.

9. Assistance to The Controller

9.1 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:

9.1.1 the right to be informed when collecting personal data from the data subject

9.1.2 the right to be informed when personal data have not been obtained from the data subject

9.1.3 the right of access by the data subject

9.1.4 the right to rectification

9.1.5 the right to erasure ('the right to be forgotten')

9.1.6 the right to restriction of processing

9.1.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

9.1.8 the right to data portability

9.1.9 the right to object

9.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

9.2 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:

9.2.1 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;

9.2.2 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;

9.2.3 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);

9.2.4 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 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

10.1 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.

10.2 The Processor's notification to the Controller shall, if possible, take place within immediately and no later than 24 hours after the processor has become aware of the breach of the personal data security 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.

10.3 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:

10.3.1 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;

10.3.2 the likely consequences of the personal data breach;

10.3.3 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.

10.4 The parties shall define in Appendix C 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 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 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:

11.2.1 we are required to continue to store information cf. the logging executive order and the Bookkeeping Act after the termination of the Data Processor 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 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 applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in C.7 .

12.3 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

13.1 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

14.1 The Clauses are binding upon the Parties.

14.2 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.

14.3 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.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned 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 The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence.

15. The controller and the processor contacts/contact points

15.1 The Parties may contact each other using the following contacts/contact points

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

Contact information for The Controller:
The to any applicable contact information, which was received at the conclusion of the contract and through ongoing cooperation.

Contact information for The Processor:
Carsten Thomsen
dpo@dstny.dk

Appendix A Information about the processing

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

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

a) The processor provides cloud storage, hosting, storage, and backup to the controller.

Provision of one or more of the following services
- Mobile telephony
- IP telephony
- Internet access
- MPLS
- PBX functionality
- Integration between internal systems and Telephony
- Firewall and Security
- Call center solutions
- Voice recording
- Meeting functionality online / by telephone
- Related services to the above areas

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

2.1 The data processor uses data from the data controller in order to deliver the requested services. For example, to make it possible to search for colleagues in the telephone system (PBX), to be able to see if the colleague is free, or to enable a desired integration.

The data processor saves the necessary information to be able to bill the requested services, for example a CDR (Call Data Record) is saved for each call made, to ensure that the billing is done correctly.

If the customer has Danish telephone numbers, Dstny must, according to the Telecommunications Act (Promulgation of the Act on Electronic Communications Networks and Services) section 31, provide number information to public number information services.

2.2 Development of apps and customer portals and provision of services in relation hereto:

a) The processor provides services in relation hereto, including IT-architecture and development resources

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

3.1 name, address, phone number, e-mail, username for one or several systems, password to one or several systems, billing and accounting documents, IP-address, information about users' used device, various personal data which are recorded in connection with the delivery of the service and cannot be precisely defined, various personal data on customers' systems to which access is granted, various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof

Billing formats for calls, SMS and data (CDR files)

3.2 The Processor may process personal data about the Controller's employees in connection with the Processor's sales, marketing and product development. This processing of personal data is not covered by the Clauses, because the Processor acts as a controller regarding of this processing. Instead, reference is made to the Processor's privacy policy which can be found on the Processor's website or upon request.

4. Processing includes the following categories of data subject

4.1 current employees, former employees, customers' employees (when customers are companies)

5. The Processor’s processing of personal data on behalf of the Controller may be performed when the Clauses commence. The processing has the following duration:

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

Appendix B Authorised Sub-processors

1. Approved sub-processors

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

General sub-processors:

SuperOffice Danmark A/S (CVR-nr.:20020695)
Delta Park 46, st.
2665 Vallensbæk Strand
Denmark
Data processing: Super Office processes data for Dstny using their Customer Relationship Management solution

Microsoft Corporation (CVR-nr: 13612870)
One Microsoft Way
Redmond, WA 98052-6399
USA
Data processing: Microsoft processes data for Dstny using their document management software and Microsoft Teams

Zendesk's United States Representative:
Zendesk, Inc.
Attn: Hasani Caraway, General Counsel & Chief Privacy Officer
1019 Market Street
San Francisco, CA 94103, United States
Data processing: Zendesk processes data for Dstny using their ticketing system to handle customer service and support inquiries

Product-specific sub-processors:

Telenor A/S (CVR-nr.:19433692)
Frederikskaj 8
2450 København SV
Denmark
Data processing: Telenor processes data for Dstny using Telenor mobile telephony

OCH A/S c/o Telia Company Danmark A/S (CVRnr.: 18936909)
Holmbladsgade 139
2300 København S
Denmark
Data processing: OCH A/S runs the common number database in Denmark, and is the common reference point for exchanging information about ported telephone numbers in Denmark. Dstny uses OCH when importing and exporting telephone numbers in Denmark.

Dateltek ApS (CVRnr.: 31060559)
Birkevej 4
4640 Faxe

Denmark
Data processing: Dateltek processes data for Dstny using their ICH system for handling number porting processes. The ICH system is only used for numbers on Telenor's network.

NPS.TODAY ApS (CVRnr.: 36464917)
Bredgade 41, 2. tv.
1260 København K
Denmark
Data processing: NPS.TODAY processes data for Dstny using the product Net Promoter Score - SMS Survey.

1.2 The Processor has the Controller's general authorisation for the engagement of sub-processor(s) from the above list. The Processor shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the data exporter to exercise its right to object.

Appendix C Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

1.1 Delivers Telephony, network and PBX functionality to the Data responsible.

2. Security of processing

2.1 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 leve 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:

Security
The Processor shall implement the following security measures:

3. Assistance to the Controller

3.1 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:

3.1.1 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.

3.1.2 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.

3.1.3 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.

4. Storage period/erasure procedures

4.1 Upon termination of the provision of personal data processing services, the Processor shall either delete or return 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.

5. Processing location

5.1 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 sub-processors as specified in Appendix B.

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

6.1 Personal data is only being processed by the Processor on the locations specified in clause C.5. 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.

6.2 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), as contained in Appendix E. 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 as contained in Appendix E under the appropriate module.

6.3 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.

6.4 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.

6.5 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.

6.6 Where, in accordance with these clauses, The Processor transfers personal data to sub-data 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.

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

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

7.1.1 is complying with his obligations under these Clauses and the Instruction, and

7.1.2 with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Controller.

7.2 According to Clause C.7.1 The Processor's documentation shall be sent to the Controller within a reasonable time after receiving the request.

7.3 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 Common Strategic Framework (CSF) - 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. In order to cover the The Data Controller's need for insight and assurance of the Data Processor's secure processing of the personal data, The Data Processor must audit The Data Processor's compliance with the the Clauses every 18 months, including the specified implemented security measures, by an external independent third party and send the complete records to the Data Controller.

7.4 Regardless of Clause C.7.3, 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 30 calendar days.

Appendix D The Parties' terms of agreement on other subjects

1. Note on the procedure for the Data Controller's audits in Annex C point 7

1.1 According to our documentation for compliance with the Data Processor agreement, reference is made to the procedure in Annex C point 7.3, as it will not be possible in practice to carry out a physical inspection of our data centres.

2. Update of the Data Processing Agreement

2.1 It is always the latest version of the data processing agreement that applies between the parties, see https://dstny.dk/databehandleraftale.

The data processor reserves the right to continuously make changes to, including clarifications of, the agreement.
These changes will typically be a result of new recommendations from e.g. The Danish Data Protection Authority or the EU Commission as well as changes in practice and legislation in the area.

The Data Controller is therefore encouraged, to sign up to receive notifications, when there are changes to the agreement:
https://dstny.dk/databehandleraftale

After receiving a notification about a change, the Data Controller has 14 working days to object, if the change cannot reasonably be accepted.

This provision does not apply to changes in the use of sub-processors, which are regulated in section 7 of the agreement.

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

Regarding transfer of personal data to the 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 fulfillment of the services specified in Clause 2.3 of 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 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 Controller to the Processor, where the Controller is not acting as a processor for another ultimate controller.
Module Three applies to transfers of personal data from the Controller to the Processor, where Controller is acting as a processor on behalf of another ultimate controller.
Module Four applies to transfers of personal data from the Processor to the Controller, where the Controller is based in a third country outside the EU/EEA, not subject to an adaquacy decison on the basis of GDPR, Article 45.

SECTION I

1. Purpose and scope

1.1 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.

1.2 The Parties:

1.2.1 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

1.2.2 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').

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

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

2. Effect and invariability of the Clauses

2.1 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), and, 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.

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

3. Third-party beneficiaries

3.1 Data subjects may invoke and enforce these Clauses, as third-party beneficiaries,

against the data exporter and/or data importer, with the following exceptions:

3.1.1 Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

3.1.2 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;

3.1.3 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;

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

3.1.5 Clause 13;

3.1.6 Clause 15.1.3, 15.1.4 and 15.1.5;

3.1.7 Clause 16.5;

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

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

4. Interpretation

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

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

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

5. Hierarchy

5.1 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.

5.2 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, Articles 46(1) and 46(2)(c).

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.

7. **Docking Clause (NOT IN EFFECT)**

7.1 ~~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.~~

7.2 ~~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.~~

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

SECTION II – OBLIGATIONS OF THE PARTIES

8. **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 ONE: Transfer controller to controller

8.1 **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. It may only process the personal data for another purpose:

8.1.1 where it has obtained the data subject's prior consent;

8.1.2 where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

8.1.3 where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

8.2.1 In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;
(ii) of the categories of personal data processed;
(iii) of the right to obtain a copy of these Clauses;
(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

8.2.2 Paragraph 8.2.1 shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

8.2.3 On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

8.2.4 Paragraphs 8.2.1 to 8.2.3 are without prejudice to the obligations of the data exporter under GDPR, Articles 13 and 14.

8.2.5 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 provisions of transparency, contained in paragraphs 8.2.1 to 8.2.4.

8.3 **Accuracy and data minimisation**

8.3.1 Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is not inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

8.3.2 If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

8.3.3 The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 **Security of processing**

8.5.1 The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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.

8.5.2 The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.5.3 The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.5.4 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 personal data breach, including measures to mitigate its possible adverse effects.

8.5.5 In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent data protection agency pursuant to Clause 13. Such notification shall contain

(i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned);
(ii) its likely consequences;
(iii) the measures taken or proposed to address the breach;
(iv) the details of a contact point from whom more information can be obtained.

To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

8.5.6 In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without

undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph 8.5.5, points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

8.5.7 The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 **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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place 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 third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

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

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 **Documentation and compliance**

8.9.1 Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

8.9.2 The data importer shall make such documentation available to the competent data protection authority on request.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

8.1.1 The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

8.1.2 The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **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 data exporter.

8.3 **Transparency**

8.3.1 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 the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses 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. This Clause is without prejudice to the obligations of the data exporter under GDPR, Articles 13 and 14.

8.3.2 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.

8.4 **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 erase or rectify the data.

8.5 **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 data exporter 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.

8.6 **Security of processing**

8.6.1 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, the Parties 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 subjects. 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. 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.

8.6.2 The data importer shall grant access to the personal 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.

8.6.3 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 the data exporter without undue delay 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 breach including, where appropriate, 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.

8.6.4 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 the competent data protection agency and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **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 described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (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

8.9 **Documentation and compliance**

8.9.1 The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

8.9.2 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 data exporter.

8.9.3 The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

8.9.4 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.

8.9.5 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 data protection agency on request.

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 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].

8.2 **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.

8.3 **Transparency**

8.3.1 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.

8.3.2 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.

8.4 **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.

8.5 **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.

8.6 **Security of processing**

8.6.1 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.

8.6.2 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.

8.6.3 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.

8.6.4 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 data protection agency and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **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.

8.8 **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

8.9 **Documentation and compliance**

8.9.1 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.

8.9.2 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.

8.9.3 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.

8.9.4 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.

8.9.5 Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

8.9.6 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.

8.9.7 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 data protection agency on request.

MODULE FOUR: Transfer processor to controller

8.1 **Instructions**

8.1.1 The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

8.1.2 The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe GDPR or other Union or Member State data protection law.

8.1.3 The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under GDPR, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

8.1.4 After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete

existing copies.

8.2 **Security of processing**

8.2.1 The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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 of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

8.2.2 The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph 8.3.1. In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

8.2.3 The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 **Documentation and compliance**

8.3.1 The Parties shall be able to demonstrate compliance with these Clauses.

8.3.2 The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

9. Use of sub-processors

MODULE TWO: Transfer controller to processor

9.1 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing

activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

MODULE THREE: Transfer processor to processor

9.1 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the

performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

10. Data subject rights

MODULE ONE: Transfer controller to controller

10.1 The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

10.2 In particular, upon request by the data subject the data importer shall, free of charge:

10.2.1 provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a data protection agency in accordance with Clause 11.3.1;

10.2.2 rectify inaccurate or incomplete data concerning the data subject;

10.2.3 erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

10.3 Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

10.4 The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to

do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

10.4.1 inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

10.4.2 implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

10.5 Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

10.6 The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in GDPR, Article 23(1).

10.7 If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

10.1 The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

10.2 The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under GDPR. 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.

10.3 In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

10.1 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.

10.2 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.

10.3 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.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under GDPR.

11. Redress

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

11.1 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.

11.2 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.

11.3 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:

11.3.1 lodge a complaint with the data protection agency in the Member State of his/her habitual residence or place of work, or the competent data protection agency pursuant to Clause 13;

11.3.2 refer the dispute to the competent courts within the meaning of Clause 18.

11.4 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).

11.5 The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6 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.

MODULE FOUR: Transfer processor to controller

11.1 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.

12. Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

12.1 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.

12.2 Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under GDPR.

12.3 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.

12.4 The Parties agree that if one Party is held liable under paragraph 12.3, 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.

12.5 The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

13.1 [Where the data exporter is established in an EU Member State:] The data protection agency 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 data protection agency.

[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 data protection agency.

[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 data protection agency 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 data protection agency.

13.2 The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent data protection agency 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 data protection agency, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

14.1 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.

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

14.2.1 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;

14.2.2 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];

14.2.3 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.

14.3 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.

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

14.5 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.]

14.6 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

15. Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 **Notification**

15.1.1 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:

15.1.1.1 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

15.1.1.2 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.]

15.1.2 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.

15.1.3 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.]

15.1.4 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.

15.1.5 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.

15.2 **Review of legality and data minimisation**

15.2.1 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.

15.2.2 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 data protection agency on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

15.2.3 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.

SECTION IV – FINAL PROVISIONS

16. Non-compliance with the Clauses and termination

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

16.2 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.

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

16.3.1 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;

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

16.3.3 the data importer fails to comply with a binding decision of a competent court or data protection agency regarding its obligations under these Clauses.

In these cases, it shall inform the competent data protection agency [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.

16.4 [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

16.5 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

17. Governing law

17.1 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.

18. Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

18.3 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.

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

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

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 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 GDPR, Article 29(3), 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 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.

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.

ANNEX I

A. LIST OF PARTIES

A.1 Data exporter:
Name:
Dstny A/S (and group-affiliated companies)
Address:
Skodsborgvej 305 D, 2850 Nærum, DK
Contact person's name, position and contact details:
Carsten Thomsen
dpo@dstny.dk

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:

Address:

Role (controller/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, paragraf 4 of the data processing agreement.

Categories of personal data transferred:
Reference is made to Appendix A, paragraf 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 from controller to controller under these clauses will not be continuous, but of a one-off nature.

Nature of the processing:
Reference is made to Appendix A, paragraf 2 of the data processing agreement.

Purpose(s) of the data transfer and further processing:
Reference is made to Appendix A, paragraf 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, paragraf 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 DATA PROTECTION AGENCY

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

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 Processor:
Reference is made to Appendix C, Clause 2 of the data processing agreement.

Technical and organisational measures taken by sub-processors:
Persuant to Clause 7.4 of the Data Processing Agreement, sub-processors must supply equivalent technical and organisational protective meassures, equivalent to those undertaken by The Processor.