STANDARD CONTRACTUAL CLAUSES

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

CVR

(the data controller) and

Neurons Inc ApS, with CVR No. 35205667

(the data processor)

each a 'party'; together 'the parties'

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

neurons

TABLE OF CONTENTS

1. PREAMBLE 3

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER 4

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS 5

4. CONFIDENTIALITY 5

5. SECURITY OF PROCESSING 6

6. USE OF SUB-PROCESSORS 7

7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS 9

8. ASSISTANCE TO THE DATA CONTROLLER 10

9. NOTIFICATION OF PERSONAL DATA BREACH 12

10. ERASURE AND RETURN OF DATA 13

11. AUDIT AND INSPECTION 13

12. LIABILITY 13

13. COMMENCEMENT AND TERMINATION 14

14. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS 15

APPENDIX A INFORMATION ABOUT THE PROCESSING 15

APPENDIX B AUTHORISED SUB-PROCESSORS 17

APPENDIX C INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA 19

APPENDIX D THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS 24

1. PREAMBLE

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

1.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.3. In the context of the provision of Neurons platform or application programming interface (API), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

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

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

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

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

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

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

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

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

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

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

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

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

documented and kept in writing, including electronically, in connectionwith the Clauses.

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

4. CONFIDENTIALITY

4.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only ona 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.

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

5. SECURITY OF PROCESSING

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

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

(a) Pseudonymisation and encryption of personal data;

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

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

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

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

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

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

additional measures to be implemented in Appendix C.

6. USE OF SUB-PROCESSORS

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

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

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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

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

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

6.5. The data processor shall agree a third-party beneficiary clause with the sub-processor wherein the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

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

7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

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

7.2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is

subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.3. Without documented instructions from the data controller, the data processor therefore can- not within the framework of the Clauses:

(a) transfer personal data to a data controller or a data processor in a third country or in an international organisation

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

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

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

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

8. ASSISTANCE TO THE DATA CONTROLLER

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

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

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

(b) the right to be informed when personal data have not been obtained from the data subject

(c) the right of access by the data subject

(d) the right to rectification

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

(f) the right to restriction of processing

(g) notification obligation regarding rectification or erasure of personal data or restriction of processing

(h) the right to data portability

(i) the right to object

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

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

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

(b) the data controller's obligation to without undue delay communicate

the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

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

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

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

9. NOTIFICATION OF PERSONAL DATA BREACH

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

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

9.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent

supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

(b) the likely consequences of the personal data breach;

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

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

10. ERASURE AND RETURN OF DATA

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

11. AUDIT AND INSPECTION

11.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and al- low for and contribute to audits,

including inspections, conducted by the data controller or another auditor mandated by the data controller.

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

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

12. LIABILITY

12.1. The data processor is only liable for the damage caused by processing in non-compliance with the data protection legislation specifically aimed at data processors; or if the data processor has failed to comply or acted in contravention of the data controller's lawful instructions.

12.2. The aggregate liability of the Data Processor for all damages, injury, and liability incurred by the Data Controller in connection with the Data Processor's Services cannot exceed to an amount equal to the amount actually paid by the Client for the Services during the immediately preceding 6 months period. Under no circumstances shall the Data Processor be liable for any consequential loss including damages for loss of profits, business interruption or other indirect pecuniary loss of any kind.

13. COMMENCEMENT AND TERMINATION

13.1. The Clauses shall become effective on the date of both parties' signature.

13.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or in- expediency of the Clauses should give rise to such renegotiation.

13.3. 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.

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

13.5. Signature
On behalf of the data controller

Name

Position

Date

On behalf of the data processor

Name Mike Storm

Position COO & Partner

Date

14. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

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

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

Name
Position
E-mail

Name Mike Storm

Position COO & Partner

E-mail: mike@neuronsinc.com

APPENDIX A INFORMATION ABOUT THE PROCESSING

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

When the Neurons Platform and application programming interface (API), which is owned and managed by the data processor, is made available to the data controller, personal data about the data controller's employees and anonymous survey participator is processed by the data processor.

The purpose of this processing is to enable the employee to access the platform provided by the data processor and run research projects using the data processor's online environment and further to enable the data controller to obtain Anonymous insights or AI Predictions to forecast customer response data.

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

The data processor receives data from the data controller based on the research projects needed. The Neurons platform then runs a data collection on anonymous survey participator or runs an analysis via the data processor AI.

The data processor platform provides a report based on the research projects setup provided by the data controller.

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

When using data processor's services, the following data is processed by data processor in the Services:

- Accounts:
  - Company name, domain, addresses, payment details
  - Usage on platform e.g. logins which incl. IP/Device data
  - Optional: Credit card

- Users:
  - Name, Email
  - Usage on platform e.g. logins which incl. IP/Device data
  - Optional data: title, phone, profile image
- Content:
  - Marketing assets e.g. video files, images, and website URLs
  - Data processor's AI predicts output

- Projects
    - Study Meta-data e.g. name, brand names, competitors
    - Anonymous participators survey data, country, age, devices, language and gender

A4. Processing includes the following categories of data subject:

- Employees: The users of our platform are employees of our customers.
- Anonymous participator: The anonymous participator of Neurons online surveys.

A5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The duration of the data processing is determined by the duration of the agreement for the provision of the data processor's Services to the data controller.

APPENDIX B AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors

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

NAME	CVR/VAT	ADDRESS	DESCRIPTION OF PROCESSING
Google Cloud		1600 Amphitheatre Parkway Mountain View, CA 94043, USA	Used as an on-demand cloud computing platforms and APIs
HubSpot		HubSpot, Inc. 25 First Street, 2nd Floor, Cambridge, MA 02141, USA	Used as a customer relationship management and support platform
Segment		Segment.io, Inc. 101 Spear Street, Fl 1 San Francisco, CA 94105 USA	Used as a data pipeline for tracking usage events in our products
Mixpanel		One Front Street, 28th Floor, San Francisco, CA 94111	Used as a data visualization tools for business and usage KPI
Sendgrid		Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105	Used as an email sending engine for Transactional emails
Stripe		Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA	Used as a payment provider for credit cards transactions
Sentry		45 Fremont Street, 8th Floor, San Fran- cisco, CA 94105	Used as a platform and infrastructure error tracking system
Weld Technologies		Weld, Frederiksholms Kanal 4, 1, 1220 Copenhagen, Denmark.	Used as for data warehouse pipelines to process and analyze data
Userflow		548 Market St PMB 69598, San Francisco, CA 94104-5401, USA	onboarding automation and for in-app notifications.

Customer.io		9450 SW Gemini Dr., Suite 43920, Beaverton, Oregon 97008-7105	email system for system email, onboarding, and re-engagement
TL;DV		Kaiser-Friedrich-Allee 51, Aachen	AI-powered meeting tool used to record, transcribe, and summarize video meetings, helping streamline internal communication and collaboration
Clerk.io		Kigkurren 8g, 2300 Copenhagen, Denmark	Used for implementation of SSO login
LinkedIn		LinkedIn Ireland Unlimited Company Wilton Place Dublin 2, Ireland	Processes customer contact and account information to provide Sales Navigator services, including data matching, insights, and CRM-based lead and account management.
Chili Piper		228 Park Ave S, #78136, New York, New York 10003-1502, United States	Facilitates efficient meeting routing and scheduling to ensure you are connected with the appropriate internal specialist
Apollo.io		440 N Barranca Ave #4750, Covina, CA 91723-1722	Used to verify and maintain the accuracy of business contact information to ensure relevant communication.
Revenue Labs		71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ	Provides internal analytics to help us evaluate and improve the efficiency of our service workflows.

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

APPENDIX C INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

- Granting employees access to the Neurons platform managed provided by the data controller. In order for the data processor's manage access and security of the platform.
- Requesting research projects with data input from data controller in order to predict the data controller's costumers' responses via anonymous participators surveys or the data processor's AI. The outcome of the data processor's processing will enable the data controller to gain data on neuroscience metrics and customer response predicts in anonymous form in a data controller's online environment.

C.2. Security of processing

The level of security shall take into account:

- That the data processor is, whenever possible, using pseudonymisation when processing personal data

The data 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 level of data security.

1. The data processor shall provide a High-availability platform and ensures application monitoring, scaling on-demand within the cloud. Ensure an SLA of 99.9%

within a calendar year.

2. The data processor shall provide a secure platform by ensuring multi-tenancy, closed-loop data access, encrypt at rest, encrypt data in transit, and fully with Audit trails to ensure the data controller data. The data processor shall ensure that all personal data and content are secured backed up in multiple data centres daily for recovery purposes.

3. The data processor shall ensure that the business continuity plan and incident management process are up to date, documented, and tested. Providing The data controller with a notification system when an incident occurs, and a historical audit trail.

4. The data processor shall inform the data controller without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of personal data detected during verification of the results of such Processing.

5. The data controller shall, upon termination or expiration of the ToS and by way of issuing an Instruction, stipulate, within a period of time set by the data Processor, the reasonable measures to return data carrier media or to delete stored data.

6. Any additional cost arising in connection with the return or deletion of personal data after the termination or expiration of the ToS shall be borne by the data controller.

C3. Assistance to the data controller

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

The data controller has access to the personal data processed by the data processor, and the data con- troller thereby has, as a starting point, the opportunity to independently take measures for handling re- quests from the data subjects in accordance with Clause 8.1. The data processor assists the data con- troller herewith to the extent necessary.

The data processor ensures procedures enabling timely assistance to the data controller in accordance with Clause 8.2.

C.4. Storage period/erasure procedures

Personal data is stored until it is marked for deletion by the data controller after which the personal data is automatically erased by the data processor.

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

C.5. Processing location

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

- Google Cloud: us-central1-a, Iowa United States
- HubSpot: Amazon Web Services, United States
- Segment: Amazon Web Services, Multiple data center locations, United States
- Mixpanel: Amazon Web Services, United States
- Sendgrid: Amazon Web Services, Multiple data center locations, United States
- Stripe: Amazon Web Services, Multiple data center locations, United States
- Sentry: Google Cloud, Multiple data center locations, United States
- Weld Technologies, Denmark.

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

By entering into this data processing agreement, the data controller agrees that the data processor transfers personal data to and stores personal data in third countries to the extent necessary using the sub-data processors listed in Appendix B.1.

The data processor uses the EU Commission's Standard Contractual Clauses as a basis for the transfer of personal data to third countries. The data controller authorizes the data processor to enter into the EU Commission's standard contractual provisions with sub-data processors in third countries in accordance with Annex D.2.

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

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

General inspection:

Once a year, data processor issues a statement of warranties and representations regarding the data processor's compliance with the obligations laid down in Article 28 of the GDPR, cf. Article 28 (3) (h) of the GDPR. The documentation is issued in May.

The statement has due regard to the risk of varying likelihood and severity for the rights and freedoms of the data subjects under this data processor agreement and includes for example the data processor's procedures to assist the data controller with the controller's obligations as agreed in this data processor agreement and data processor's technical and organisational security measures relevant to this data processing agreement.

Extra documentation:

Apart from this planned statement of warranties and representations, the data controller may request extra documentation for compliance with the data processor's obligations in Article 28 of the GDPR to the extend the data processor's said statement of warranties and representations does not cover the matters on which the data controller requests further documentation.

Regard being had to the risks of the data subjects and the described inspection, the parties agree that the total inspection frequency is once a year.

Physical inspection:

The data controller or the data controller’s representative may no more than once a year perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for the processing to ascertain the data processor’s compliance with the GDPR, the applicable EU or Member State data protection provisions and this data processor agreement.

The data controller’s costs, if applicable, relating to physical inspection shall be defrayed by the data con- troller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

Once a year, data processor provides data controller with documentation regarding the sub-processors' compliance under this agreement. The documentation is issued in May.

The documentation from sub-processors may vary according to their risk profile and ability to provide. For the time being, the following documentation is issued:

Data Processor has entered into separate data processing agreements with the sub-processors. These agreements contain adequate provisions regarding a compliance audit.

The audit of sub-processors is taken place and will be taken place pursuant to these clauses.

APPENDIX D THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

D.1. Compliance with Clause 7.6.

The parties agree that the data processor shall only comply with the obligation in Clause 7.6 to include the data controller as a beneficiary third party in its agreements with sub-data processors to the extent that this can reasonably be implemented vis-à-vis the relevant sub-data processors.

D.2. POWER OF ATTORNEY

D.2.1. INTRODUCTION

By entering into this data processing agreement, the data controller agrees that the data processor transfers personal data to and stores personal data in third countries to the extent necessary using the sub-data processors specified in Annex B.1.

D.2.2. SCOPE OF POWER OF ATTORNEY

By signing this data processing agreement, the data controller authorises the data processor to enter into the agreements necessary for the transfer of personal data to third countries. The purpose is to ensure an adequate level of protection for the

personal data which the data controller has left for processing by the data processor in accordance with the Clauses.

The power of attorney includes the conclusion of the EU Commission's Standard Contract Clauses on be- half of the data controller, so that the standard contract provisions apply directly to the data processing carried out by one or more Sub-data processors established outside the EEA and adopted by the data processor on behalf of the data controller.

The power of attorney only includes the conclusion of the standard contract provisions in unchanged form.

D.2.3 OTHER

The data processor cannot give the power of attorney to a third party. The power of attorney is subject to Danish law.

D.3 Assistance to the data controller and extra documentation

The data processor's assistance to the data controller in accordance with Clause 9 and regarding "extra documentation" in Clause C.7 and C.8 is remunerated separately according to the Parties' agreement. The remuneration is calculated on the basis of the data processor's hourly rates and expenses incurred for external assistance, including from sub-data processors or advisers.

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

*Information Security Policy can be sent on request