Data Processing Agreement

Adversus A/S

Data Processing Agreement

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

between

Company name:
Business Reg. No.:
Address:

(the data controller)

and

Company name: Adversus A/S
Business Reg. No.: 37831247
Address: Karupvej 2D, 3. tv.
8000 Aarhus C
Denmark

(the data processor)

each a 'party' ; together 'the parties'

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

1. Table of Contents

2. Preamble

1. This Data Protection Agreement (the DPA) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

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

3. In the context of the provision of the Adversus App Platform, the data processor will process personal data on behalf of the data controller in accordance with the DPA.

4. This Data processing agreement shall supersede all prior data processing agreements between the data processor and the data controller.

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

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

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. The data controller must be solely responsible for the correct completion of appendix A and the subsequent types of data that are uploaded and processed in the Adversus App platform.

8. 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.

9. 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.

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

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

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

3. The rights and obligations of the data controller

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

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

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

4. The data processor acts according to instructions

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

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

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has

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

been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

3. Persons under the data processor's authority, can only access data being processed in Adversus, by access granted from the data controller within the control module in the Adversus App Platform.

6. Security of processing

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

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

a. Pseudonymisation and encryption of personal data;

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

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

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

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

controller shall provide the data processor with all information necessary to identify and evaluate such risks.

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

7. Use of sub-processors

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

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

3. The data processor has the data controller's specific authorisation for the engagement of the sub-processors approved in Appendix B. The data processor may, by giving reasonable notice to the data controller, add to the Sub-processor Page. The data processor will notify the data controller if it intends to add or replace Sub-processors from the Sub-Processor Page at least 30 days prior to any such changes.

   If the data controller objects to the appointment of an additional Subprocessor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, then the data processor will work in good faith with the data controller to find an alternative solution.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the DPA 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 DPA 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 DPA and the GDPR.

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

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

8. Transfer of data to third countries or international organisations

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

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

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

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

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

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

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

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

6. If the data processor transfers data outside of EU/EEA, the data processor must assist the data controller in the preparation of appropriate documentation, including Transfer Impact Assessments, without separate remuneration.

9. Assistance to the data controller

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

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

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

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

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

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

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

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

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

10. Notification of personal data breach

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

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

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

b. the likely consequences of the personal data breach;

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

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

5. Adversus' notification of or response to a Security Breach shall not be construed as an acknowledgement by Adversus of any fault or liability with respect to the Security Breach.

11. Erasure and return of data

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

12. Audit and inspection

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

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

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

13. The parties' agreement on other terms

1. The parties may agree to 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 DPA or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The DPA shall become effective on the date of both parties' signature.

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

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

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

5. Signature

On behalf of the data controller

Name:
Position:
Date:
Signature:

On behalf of the data processor

Name: Kasper Klit
Position: CEO
Date:
Signature:

15. Data controller and data processor contacts/contact points

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

The data controller

The email address specified by the data controller in connection with its sign-up to the Adversus App Platform.

The data processor

legal@adversus.io

Appendix A: Information about processing

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

(i) the provision to the data controller of the Adversus App Platform, incl. support, maintenance, and backup.

(ii) other purposes for which the data controller instructs the data processor in writing.

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):

Storage, processing and backup of the personal data the data controller uploads to the Adversus App Platform. The Adversus App Platform enables the data controller to carry out processing activities such as systemisation, statistical data generation, and sorting according to different criteria.

A.3 and A.4. The processing includes the following types of personal data about data subjects and the following categories of data subjects:

The data controller is responsible for adhering to the rules of GDPR, relating to the types of personal data being processed. Personal data that has the nature of "sensitive data", should only be processed if the controller has ensured they are compliant with the restrictive rules set forth in the GDPR legislation, ex. but not limited to consent or the nature of the data controllers business.

Types of data subjects	Prospective customers/members
Types of personal data	Personal data uploaded by the data controller in the call center software provided by the data processor, including but not limited to name, title, address, telephone number, email, and other relevant information available to the data controller. Special categories of personal data may be processed.

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

The processing continues for as long as the personal data processing services are provided to the data controller.

Appendix B: Authorised subprocessors

B.1. Approved subprocessors

Adversus uses a number of sub-processors who act under our instructions and in certain cases may be in possession of personally identifiable data from you or your customers.

We keep track of all our sub processors and ensure appropriate measures are taken in terms of securing the processing of data through their services, including but not limited to DPA's, incorporating SCC's where necessary and adequate technical measures.

Below you can see the sub-processors that Adversus uses. They are divided into sub-processors that either process data within the EU and the EEA or sub-processors where there is a risk that data will be processed outside the EU and the EEA.

In the event that a feature is critical to the data controller and can't be approved, the data processor will work with the data controller to find an alternative solution.

Sub-processors processing data within the EU/EEA

System requirement	Subprocessor	Description of product	Purpose	Data processing location	Approved by data controller
Required	DLX A/S	Operation of Adversus platform app (backend)	Primary operation server for the system.	Hammershusvej 16C, 7400 Herning Denmark	N/A
Optional	OVH Cloud	Storage of recorded conversations	When recording conversations according to the customer's choice of setting, these would be stored at OVH. Adversus is only using data centers in the EU and recordings will never be processed outside the EU/ EEA. The function only processes data, upon activation.	France	☐ Yes ☐ No
Required	Flowmailer	Controls the internal email functiona-lity within the Adversus App Platform.	Handling of all the required email functionality within the platform. This could be resetting passwords for users, exporting data, inviting users etc.	Netherlands Van Nelleweg 1, 3044BC Rotterdam, The Netherlands	N/A

Sub-processors that might process data outside the EU/EEA

System requirement	Subprocessor	Description of product	Purpose	Data processing location	Approved by data controller
Optional	SessionStack	Screen Sharing inside the Adversus App Platform.	Helping customers in the Adversus app platform with playback sessions of latest interactions, focusing on problem identification and solving. Activation of this service will result in the transfer of data outside the EU/EEA. Whenever possible, Adversus will always ask a sub-processor to use a setup that is within the EEA for processing of personal data, and ensure that the correct SCCs are implemented, when transfer out-side EU/EEA can occur. The function only processes data, upon activation.	Germany	☐ Yes ☐ No
Optional	SureSMS	SMS service enabling the SMS function in Adversus App.	Send SMS messages to the customer directly via the Adversus App. Activation of this feature could result in the transfer-ring of data outside EU/EEA. SureSMS are using AWS and though all protective measures have been taken in regards to protecting personal data, if com-pelled by foreign legislation, personal data could be subject to transfer ex. to the US. Whenever possible, Adversus will always ask a sub-processor to use a setup that is within the EU/EEA for processing of personal data, and ensure that the correct SCCs are implemented, when transfer out-side EU/EEA can occur. The function only processes data, upon activation.	Germany	☐ Yes ☐ No
Optional	Cronofy	App for managing calendar planning.	Calendar Function which can integrate against different calendar platforms, e.g., Google calendar. Activation of this feature could result in the transfer-ring of data outside EU/EEA. Cronofy are using AWS and though all protective measures have been taken in regards to protecting personal data, if com-pelled by foreign legislation, personal data could be subject to transfer ex. to the US. Whenever possible, Adversus will always ask a sub-processor to use a setup that is within the EU/EEA for processing of personal data, and ensure that the correct SCCs are implemented, when transfer out-side EU/EEA can occur. The function only processes data, upon activation.	Germany	☐ Yes ☐ No

Optional	Sendgrid (Twilio)	Controls the external email functionality within the Adversus App Platform.	Sending email to customers through the system, e.g., appointment confirmations. Activation of this service will result in the transfer of data outside the EU/EEA. Whenever possible, Adversus will always ask a sub-processor to use a setup that is within the EU/EEA for processing of personal data, and ensure that the correct SCCs are implemented, when transfer outside EU/EEA can occur. The function only processes data, upon activation.	US	☐ Yes ☐ No
Optional	Google Affiliate Service	Controls the Google Maps functionality inside the Adversus App Platform.	Address lookup function through Google Maps. Using this function could result in the transferring of personal data outside EEA - same principles as when using Google Maps privately. Whenever possible, Adversus will always ask a sub-processor to use a setup that is within the EU/EEA for processing of personal data, and ensure that the correct SCCs are implemented, when transfer outside EU/EEA can occur. The function only processes data, upon activation.	Ireland	☐ Yes ☐ No

Operational Software

In addition we use a range of standard operational software, in which personal data might also get processed. The suppliers and their setup in relation to personal data has been examined, assessed and accepted as being sufficient in relation to compliance with GDPR.

System requirement	Subprocessor	Description of product	Purpose	Data processing location	Approved by data controller
Required	Intercom	Customer service platform	Communication by chat/email service with customer service. Adversus is using the EU-setup Intercom is running and has signed an Addendum, in order to ensure compliance with legislation regarding data transfer to third countries.	Ireland	N/A
Required	Flexfone	Internal telephony system.	Covering usage on internal phones and customer support.	Denmark	N/A
Required	Google Workspace	Workspace system	Collective workspace and operation space. Utilizing Docs, Sheets Drive, mail etc.	Ireland Grange Castle Business Park South, 22 Baldonnel Rd, Dublin 22, D22 X602, Ireland	N/A

Operational Partners

System requirement	Subprocessor	Description of product	Purpose	Data processing location	Approved by data controller
Optional	WOW 24-7	External customer support. Outside normal opening hours (08-22 CET).	Provide customer support outside regular business hours. All data is still stored within systems controlled by Adversus and WOW 24-7 is not a data processor in the traditional sense. WOW 24-7 are under strict NDA, placing them under the same strict legal confidentiality that our own employees have signed.	Cyprus	☐ Yes ☐ No

The data controller shall on the commencement of the DPA authorise the use of the above-mentioned sub-processors checked with a “yes” for the processing described for that party.

The data processor shall inform the data controller of any changes concerning the addition or replacement of sub-processors, in accordance with Clause 7.3.

Appendix C: Instruction pertaining to the use of personal data

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

The data processor provides to the data controller the Adversus App Platform - a telecommunications system that enables the data controller to upload information on potential and existing customers and/or members for the purpose of subsequently contacting them, to market and sell the data controllers products and services. The system also allows the data controller to track its marketing and sales activities by recording information on the result of calls, call attempts, blocking lists and the interests expressed by the data subjects in the data controller's products and services. The data uploaded to and subsequently recorded by the data controller in the Adversus App Platform is stored and back-uped by the data processor.

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:

Data processing related to the provision of the Adversus App Platform. The data processor is entitled to process the personal data to the extent necessary for the provision of the service by the data processor.

The data controller shall regularly transmit to the data processor the statistical data generated in connection with the use of the service. The information is transmitted to the data processor as anonymised statistical information and no personal data is thus transmitted to the data processor.

C.2. Security of processing

The level of security shall take into account:

The processing involves a large volume of personal data subject to Article 6 GDPR and there is a chance that personal data subject to Article 9 GDPR is also processed.

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 (and agreed) level of data security.

The data processor shall however – in any event and as a minimum – implement the following measures that have been agreed with the data controller:

Anonymisation or deletion of data either by the data controller performing the task, or by the data processor performing the task according to instruction from the data controller. Insofar the system

does not support the task being performed by the data controller itself, the data processor is not entitled to be remunerated separately for its performance of the task.

Ensure restoration of access to personal data within 72 hours.

Logging with unique user-identification. The logfile is retained for a minimum of 180 days. The log contains information on log-in/log-out and records accessed.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible assist the data controller in accordance with Clause 9.1. and 9.2.

The data processor's services in relation to this clause C.3 shall be remunerated separately, in accordance with Annex D, clause 3.

C.4. Storage period/erasure procedures

Personal data is stored for as long as the personal data processing services are provided to the data controller. Hereafter the data is stored for 1 month, after which it will be permanently deleted.

The deletion of personal data does not include personal data stored in backup. The personal data stored in backup is deleted in accordance with the data processor’s normal backup cycle. The backup-cycle is 3 months, after which the personal data will be permanently deleted.

Data that is necessary in order to meet the conditions relating to Danish accounting legislation will be stored for the required 5 years, this does not include personal data.

C.5. Processing location

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

The locations listed in Appendix B, clause B.1.

The data processor shall notify the data controller of any changes concerning the processing location in accordance with the procedure set out in Clause 7.3. If the data controller does not object to such changes, the data controller shall be deemed to have approved the change. The data processor shall

only be obliged to comply with the data controller's objection under Clause 7.3 if the data controller's objection contains compelling objective reasons against the application of the intended change in the processing location.

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

The data processor has the data controllers authorisation for the transfer of personal data to third countries, in accordance with the subprocessor list set forth in Appendix B, approved by the data controller.

The subprocessor list will be specified regarding location of processing and the functionality which each subprocessor performs in the Adversus App platform.

The data controller is solely responsible for instructions given to the data processor regarding which functions must be activated on the Adversus App platform and therefore also which sub processors that are processing data.

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

The data controller or a representative of the data controller has the right to audit the processing of personal data carried out by the data processor on behalf of the data controller. Where the audit is carried out by someone other than the data controller itself, that representative shall be independent and non-competitive of the data processor.

The parties agree that the data controller’s audit shall, as a main rule, be carried out as a written audit. However, the data controller may, in addition to the written audit, with at least 3 months' prior notice, conduct a physical inspection at the data processor's premises if the data controller due to specific circumstances exceptionally deems it required.

The data processor's services in relation to this clause C.7 shall be remunerated separately, in accordance with Annex D, clause 3.

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

The data processor shall, at its own expense, perform audits/inspections of the processing of personal data being performed by sub-processors to ascertain the sub-processor’s compliance with

the data processing agreement concluded between the data processor and the sub-processor. The frequency and the type/content of the audit/inspection is determined by the data processor in accordance with its policy on sub-processor audits.

Appendix D: The parties' terms of agreement on other subjects

D.1. Transfer of data to third countries

1. If the transfer basis used requires the data controller to be a direct party thereto, the data processor is authorised to enter into this on behalf of the data controller, for example by concluding the contract using the EU Commission's Standard Contractual Clauses, with the necessary supplementary measures for compliance with the GDPR, on behalf of the data controller. The data processor shall inform the data controller as soon as possible if this authorisation is exercised.

2. The regulation applicable under the employed transfer basis shall prevail over the regulation in this DPA, but only in relation to the processing which necessitates the transfer basis; other processing shall be governed solely by this DPA.

D.2. Use of sub-processors

1. The data processor shall only be obliged to comply with the data controller's objection under Clause 7.3 if the data controller's objection contains compelling objective reasons against the application of the intended amendment concerning the addition or replacement of sub-processors.

2. The data controller agrees that the processing of personal data on behalf of the data controller by sub-processors shall be carried out in accordance with the terms and conditions laid down in the standard terms and conditions of that sub-processor in force from time to time, where the data controller has been informed of this. Such information regarding sub-processors can be found in the list of sub-processors in Appendix B, Clause B.1.

D.3. Remuneration

1. The data processor is obliged, without additional charge, to help the data controller comply with his obligations according to the GDPR regulations. For activities that go beyond the minimum requirements set out in the GDPR legislation, the data processor will be entitled to remuneration.

2. The fee shall be calculated according to the data processor's applicable hourly rates.

3. Notwithstanding the above, the data processor shall not be entitled to payment for assistance or implementation of changes to the extent that such assistance or change is a direct result of the data processor's own breach of the DPA.

D.4. Liability and limitations of liability

1. The data controller is aware that the data processor is dependent on the data controller's instructions as to the extent to which the data processor is entitled to use and process the personal data on the data controller's behalf. The data processor shall therefore not be liable for any claims arising from the acts or omissions of the data processor to the extent that those acts or omissions are a direct consequence of the provision of the personal data processing in accordance with the instructions of the data controller.

2. The limitation of liability in the parties' agreement for the provision of the services relating to the processing of personal data shall apply to the processing of personal data by the data processor under this DPA, as well as with respect to Article 82(5) of the GDPR.

D.5. Assignment

1. The data processor is entitled to assign its rights and obligations under the DPA to a company affiliated with the data processor without consent.

2. The data processor shall also be entitled to assign its rights and obligations under the DPA without consent as part of a full or partial transfer of business. In the event of any such transfer, the data processor shall inform the data controller of the transfer immediately after the transfer and make the necessary adaptations to the DPA.

D.6. Commencement and termination

1. The DPA is incorporated by reference in the terms of service for the Adversus App Platform (the Service Agreement). The DPA becomes effective upon completion and signing.

D.7. Disputes and applicable law

1. This DPA shall be governed by and construed in accordance with Danish law, excluding (a) its conflict of laws rules leading to application of laws other than Danish laws and (b) the UN Convention on Contracts for the International Sale of Goods (CISG).

2. Any dispute which cannot be settled amicably shall be brought before the competent court at the data processor’s place of residence.

adversus

March 2023