

Changelog

CHANGE	VERSION
1.0.	First version published

Data Processing Agreement

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

between

Client of BeCause ApS

(the data controller)

and

BeCause ApS
CVR 39745267
Njalsgade 76,
2300 København S
Denmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Data Processing Agreement (the "DPA") in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

1. Table of Contents

2. Preamble	4
3. The rights and obligations of the data controller.....	4
4. The data processor acts according to instructions	5
5. Confidentiality	5
6. Security of processing	5
7. Use of sub-processors.....	6
8. Transfer of data to third countries or international organizations	7
9. Assistance to the data controller	7
10. Notification of personal data breach	9
11. Erasure and return of data.....	9
12. Audit and inspection	9
13. The parties' agreement on other terms	10
14. Commencement and termination	10
15. Data controller and data processor contacts/contact points.....	10
Appendix A Information about the processing	12
Appendix B Authorized sub-processors.....	13
Appendix C Instruction pertaining to the use of personal data	14
Appendix D The parties' terms of agreement on other subjects	19
Appendix E Sub-processor policies specifying transfer mechanisms and security measures	Error! Bookmark not defined.

2. Preamble

1. This 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 have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
3. In the context of the provision of services under the agreement ("the Agreement") entered into between the parties, the data processor will process personal data on behalf of the data controller in accordance with the DPA.
4. The DPA shall take priority over any similar provisions contained in other agreements between the parties.
5. Four appendices are attached to the DPA and form an integral part of the DPA.
6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.
8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
9. Appendix D contains provisions for other activities which are not covered by the DPA.
10. The DPA along with appendices shall be retained in writing, including electronically, by both parties.
11. 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.
12. Any term not defined in the DPA shall have the meaning set out in the GDPR.

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 State¹ data protection provisions and the DPA.

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

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 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.

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 organizational 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. Pseudonymization 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 organizational 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 organizational 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 requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the prior general written authorization of the data controller.
3. The data processor has the data controller's general authorization 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 thirty (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 authorized by the data controller can be found in Appendix B.
4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the 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 organizational 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 organizations

1. Any transfer of personal data to third countries or international organizations 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 organizations, 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 in 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.

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 organizational 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 subjects
 - c. the right of access by the data subjects
 - 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, namely the supervisory authority in the country in which the data controller is established, for example Datailsynet (Danish Data Protection Agency) in Denmark, 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, namely the supervisory authority in the country in which the data controller is established, 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 organizational 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 twenty-four (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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall subject to the data controller's instruction be under obligation to either (i) delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or (ii) return all the personal data to the data controller and delete existing copies 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 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 Clauses governing the provision of personal data processing services have been agreed between the parties.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the DPA may be terminated by written notice by either party.
5. Signature

On behalf of the data processor

Name	Jonas Bruun Jacobsen
Position	Chief Technology Officer
Date	
Signature	

15. Data controller and data processor contacts/contact points

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

Company	BeCause ApS
Name	Jonas Bruun Jacobsen
Position	Chief Technology Officer
Telephone	+45 7179 4220
E-mail	Jonas@because.eco

In case of a data breach, the following e-mail must be used: privacy@because.eco

Name	Jonas Bruun Jacobsen
Position	Chief Technology Officer
Telephone	+45 7179 4220
E-mail	Jonas@because.eco

Appendix A Information about the processing

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

The data processor is processing personal data on behalf of the data controller for the purpose of providing the services agreed between the parties under the Agreement.

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 nature of processing carried out under the Agreement in accordance with these DPA, will involve:

- Data storage
- Back-up
- User support
- Service messaging
- Communicational messaging upon order from data controller

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

- Name
- E-mail address
- Telephone number
- Username
- IP address
- Job title
- Company name (included as personal data in case of single person company)
- CVR or VAT ID (included as personal data in case of single person company)

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

The categories of data subjects are the identified or identifiable natural person whose personal data is being processed under the DPA, e.g.:

- Employees of the data controller
- Employees employed at customers of the data controller

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

The term of this DPA shall continue until the latter of the following; the termination of the Agreement, or the date at which the data processor ceases to process the personal data.

Appendix B Authorized sub-processors

B.1. Approved sub-processors

On commencement of the DPA, the data controller authorizes the engagement of the following sub-processors:

Sub-processor	Address	Description	Location of data stored	Transfer mechanisms & security measures	Applicable BeCause services
Microsoft Azure	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Data hosting provider	Data residency located in Republic of Ireland and Netherlands.	SCC + encryption (among other measures)	Applicable to all BeCause services.
Microsoft Office 365	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Documents provided over email by the data-controller will be stored on Cloud Microsoft Exchange servers provided by Microsoft as part of their Office 365 offering	European Union	SCC + encryption (among other measures)	BeCause email servers, Microsoft Teams chats, Onedrive hosted documents
Sparkpost	160 Old Street, London, EC1V 9BW	Mails are sent through Sparkpost to the customers on the platform, if settings or action is triggered to do so by a representative of the data controller.	No data stored with sparkpost. Mail-addresses can have names though that can identify unique users. Sparkpost processes the mails within EU https://www.sparkpost.com/gdpr/ .	SCC + encryption (among other measures)	Applicable to all automated non-marketing BeCause emails.

The data controller shall on the commencement of the DPA authorize 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 authorization in accordance with Clause 7 – to engage a sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Monitoring of sub-processors

Where the data processor is entitled to assign processing of personal data under this DPA to a designated sub-processor, the data processor shall:

- check in advance and then on a regular basis whether the sub-processor(s) has taken the necessary technical and organizational security measures and is acting in accordance with the DPA; and
- ensure that the data controller is granted the right to monitor and inspect the documentation and certification provided by the data processor about its sub-processor in accordance with this DPA and the GDPR and applicable national data protection legislation. Upon the data controller’s written request, the data processor will provide written confirmation of the imposition of data protection regulations on the sub-processor no less restrictive than those agreed in this DPA between the data controller and the data processor.

B.3. Termination due to changes to or engagement of sub-processors

Data controller shall be entitled to immediately terminate this DPA fully or partly for convenience and without incurring any termination fees, if the data processor:

- fails to give written notice to the data controller as specified in Clause 7.3. of the DPA;
- fails to comply with the requirements set out in section 2.b above, or
- proceeds with any intended changes concerning the addition or replacement of sub-processors despite the data controller objecting hereto.

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 as part of providing the agreed services, as specified in Appendix A.

C.2. Security of processing

Taking into account the nature, scope, context, and purposes of processing as set out above, as well as the risks for the rights and freedoms of the data subjects, the following elements have been taken into account when assessing the security of processing:

- The processing involves systematic monitoring including processing used to observe, monitor or control data subjects
- The processing involves matching or combining dataset
- The processing involves innovative use or applying new technological or organizational solutions
- The processing involves automated decision making with legal or similar significant effect
- The processing involves evaluation or scoring including profiling and predicting

The data processor must ensure that appropriate aspects of good security practices are implemented when processing personal data on behalf of a data controller, which may include the following measures:

C.2.1. Organizational security

- The data processor maintains and enforces policies on handling data securely and to ensure personal data is processed in accordance with applicable law. The data processor takes appropriate steps to ensure that such policies are known to all employees through regular awareness training.
- The data processor ensures that third party service providers adhere to a minimum set of controls prescribed by the data processor and are made subject to confidentiality obligations prior to engagement.
- The data processor regularly audits third party services and sub-processors based on risk in the processing of personal data.
- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing the data processor will implement and adhere to the data protection by design principles in all phases of the data and system life-cycle.

C.2.2. Physical Security

- Personal data that is stored on sites controlled by the data processor, including data centers, offices and off-site storage facilities have appropriate physical security controls.

C.2.3. System and Network Security

- Networks and devices on which personal data are processed, are protected from unauthorized access or infiltration, both internally or externally.
- Network security is maintained by the use of commercially available equipment and industry standard techniques, including periodic external vulnerability scanning are conducted and perimeter defenses such as firewalls and intrusion prevention/detection systems are maintained.
- Internal defenses such as security information event management, which can analyze log files can detect anomalous behavior and threats.
- The infrastructure must be segmented to at least separate production systems from test and development environments.
- Anti-virus and anti-malware systems used on operating systems together with secure configuration. Vendor recommended security patches applied in a timely fashion for both applications and operating systems.
- Encryption used on laptop hard drives and portable media, as required.
- Risk assessments performed and documented using industry accepted methodologies.

C.2.4. Data confidentiality

- Data processed by the data processor on behalf of the data controller will be maintained by protection both in storage and in transmission of the data.
- Protection is ensured through access limitation, so that access is limited to only those who have a business need.
- Protection of data in transmission is also ensured by encryption when transmitting data via open networks.
- The data processor also ensures secure disposal of data, media, equipment, and paper.

C.2.5. Data access

- The data processor ensures that the data controller's personal data is only accessed by authorized persons, through the means of access management procedures that ensure access on a least privilege basis and that access is terminated where and when it is appropriate.
- The data processor must perform regular controls of the assigned rights. The controls must be documented.
- Systems used to process the data controller's personal data is further secured through multiple factor authentication.

C.2.6. Logging

- All login attempts must be logged in order to detect unauthorized access to personal data.
- All access to personal data must be logged and the access log must include the date and time of access, the UserID and the type of access (read, edit, delete, search criteria etc.).
- Security logging must be enabled on all network equipment, servers and on all applications including databases and on IT system administrators.

- Logs of access to personal data and the use of personal data must be monitored and regularly reviewed by the data processor in order to detect unauthorized access to personal data.
- The data processor must have a documented procedure for how often log files are reviewed and who has performed the control. Documentation must be made available to the data controller on request.

C.2.7. Back-up

- The data processor must perform back-up of the personal data processed on behalf of the data controller and must have procedures in place to ensure the re-establishing of backed-up data in a timely manner to ensure the availability and access to personal data.
- The data processor must have a documented procedure for performing backup. Such procedure must identify data retention and data deletion requirements.
- Backups must be protected from unauthorized access including destruction and must be encrypted if the back-up contains any personal data where encryption based on a risk assessment is required.

C.2.8. Availability

- The data processor must implement procedures for effective detection, analysis and handling of security events to ensure the availability of personal data.
- The data processor must implement a documented and tested disaster recovery plan and business continuity strategy covering systems used to process personal data.
- Disaster recovery plans and business continuity strategies must be tested and updated regularly, and at least annually, to ensure that they are up to date and effective. Documentation must be made available to the data controller upon request.

C.2.9. Data processing

- The data processor maintains and enforces policies on handling data securely, and takes appropriate steps to ensure that such policies are known to all employees through awareness training.
- The data processor ensures that third party service providers adhere to a minimum set of controls prescribed by the data processor and are made subject to confidentiality obligations prior to engagement.

C.3. 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 organizational measures:

The data processor has in place policies and procedures to ensure that appropriate aspects of good security practices are enforced so that the data processor is able to assist the data controller in a timely fashion, including ensuring that the data subjects' rights are met.

The data processor has established and will maintain procedures and technical features in the IT systems used in the provision of the services that will allow the data processor, upon request from the data controller, to (i) identify personal data related to data subjects in order for the data controller to accommodate data subject access requests, (ii) rectify or delete personal data recorded and (iii) restrict further processing of personal data.

C.4. Storage period/erasure procedures

Personal data is stored for the period of time agreed in the service description or as instructed by the data controller from time to time 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 DPA.

Deletion shall take place without undue delay and no later than thirty (30) days from the data controller's request. Upon the data controller's written request for certification of deletion, the data processor shall certify in writing the deletion of the personal data and any copies thereof.

C.5. Processing location

Processing of the personal data under the DPA cannot be performed outside the EU/EEA without the data controller's prior written authorization. Currently the processing is performed at the locations specified in Appendix B.

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

The data processor and its sub-processor(s) (if any) must not transfer personal data out of the EU/EEA without the prior written approval of the data controller. In the event such approval is granted, the data processor must comply with any requirements established by any supervisory authority or any other governmental authorities necessary for the granting of approval by such authorities for the transfer of personal data outside of the EU/EEA, including by adherence to the Commission's standard contractual clauses as set out by Commission Implementing Decision (EU) 2021/914 of June 4, 2021, with later amendments, to the extent applicable.

Upon written approval from the data controller the data processor shall ensure the legal basis for the transfer of personal data either by way of (a) the third country being a jurisdiction on the list of the European Commission with jurisdictions that provide an adequate level of data protection, (b) the third country being a party to a certification scheme approved by the European Commission as providing the adequate level of data protection or (c) procuring that the sub-processor enters into the European Commission's Standard Contractual Clauses for the transfer of personal data to the sub-processor established in third countries. The data processor and its sub-processor(s) (if any) will not be entitled to require any amendments to the Commission's Standard Contractual Clauses. The data controller authorizes the data processor to execute the European Commission's Standard Contractual Clauses for the transfer of personal data to sub-processors established in third countries on behalf of the data controller.

In the event that a legal basis for transfer of personal data as set out in this Article C.6 is found non-compliant with the applicable data protection legislation and is replaced or otherwise no longer considered to be the foundation for a valid legal basis for the transfer of personal data out-side of the EU/EEA the Parties will together without undue delay find and execute another legal basis for the transfer of personal data out of the EU/EEA.

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

Upon the data controller's written request, the data processor shall within sixty (60) days at the data controller's expense either provide to the data controller an audit report covering control of the technical and organizational security measures implemented by the data processor which will be prepared by an independent third party that attests to the compliance of the applicable security controls, or complete a security questionnaire submitted by the data controller to the data Processor.

The audit report or security questionnaire shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit under a revised scope and/or different methodology.

Based on the results of such an audit, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. 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 performed by sub-processors

Upon the data controller's written request, the data processor shall within sixty (60) days at the data controller's expense either provide to the data controller an audit report covering control of the technical and organizational security measures implemented by the sub-processor which will be prepared by an independent third party that attests to the compliance of the applicable security controls, or have the sub-processor complete a security questionnaire submitted by the data processor to the sub-processor.

Documentation for such audit report or security questionnaire shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit under a revised scope and/or different methodology.

Based on the results of such an audit, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

Appendix D The parties' terms of agreement on other subjects

D.1. Additional responsibilities of the data processor

The data processor also undertakes

- to notify the data controller without undue delay of any monitoring activities and measures undertaken by a supervisory authority pursuant to the GDPR and applicable national data protection legislation. This also applies where a competent authority investigates the data processor and sub-processor(s) (if any) in accordance with the GDPR and applicable national data protection legislation;
- to monitor the processing of personal data by regular reviews by the data processor of the performance and fulfilment of this DPA, particularly compliance with and any necessary amendment to provisions and measures laid down to carry out the obligations under this DPA;
- to provide with full cooperation and assistance in relation to any complaint or request made;
- to provide the data controller within no more than seven (7) days of a written request of the data controller with detailed information on the current location of any personal data being processed or stored by the data processor and its sub-processor (if any); and
- to notify the data controller in writing within seven (7) days if it receives (i) a request from a data subject to have access to that person's personal data; or (ii) a complaint or request relating to the data controller's obligations under the GDPR and applicable national data protection legislation.

D.2. Data Breach Notification

The notification to the data controller from the data processor of a personal data breach must at least

- describe the personal data breach including the categories and number of data subjects concerned, date and time of the incident, summary of the incident that caused the personal data breach, the categories and number of data records concerned, and the nature and the content of the personal data concerned;
- describe the circumstances of the personal data breach (e.g. loss, theft, copying);
- communicate the identity and contact details of the data processor's data protection officer or other contact point where more information can be obtained;
- recommend measures to mitigate the possible adverse effects of the personal data breach;
- describe the likely consequences and potential risk to the data subject due to the personal data breach;
- describe the measures proposed or taken by the data processor and/or the sub-processor, as applicable, to address the personal data breach;
- include any other information required in order for data controller to comply with the GDPR and applicable national data protection legislation, including duties of notification and disclosure in relation to public authorities.

D.3. Liability and indemnification

The data processor shall hold the data controller fully and effectively indemnified against any and all claims, expenses, losses and damages or liabilities suffered by the data controller aris-

ing from the data processor and sub-processor(s) (if any) not fulfilling its data protection obligations under this DPA. The data processor cannot limit or exclude the data controller's right to claim and the data processor's obligation to indemnify in accordance with this clause D.3 due to breach of the data protection obligations set out in DPA.

Regardless of any previous provisions to the contrary set forth elsewhere between the Parties, the following losses shall always be regarded as direct losses:

- costs and expenses of restoring or reloading any lost, stolen, or damaged data resulting from a default by the data processor;
- costs and expenses related to the management of a breach of the data protection legislation and/or the DPA, including administrative costs, forensic investigations, and communications;
- loss resulting from compromising or intrusion of the data controller's network through an intrusion of the data processor's network or through an unauthorized access by the data processor's personnel; and
- regulatory fines, penalties, sanctions, interest or other regulatory monetary remedies incurred by the data controller as a result of the data processor's failure to comply with the data protection legislation that the data processor is obliged to comply with; to the extent that the decision and calculation of the fines are based on circumstances within the data processor's control. The data controller shall immediately notify the data processor of any such regulatory remedies and shall upon the data processor's request grant the data processor authorization to on behalf of the data controller, to appeal such decision to higher authorities.

D.4. Choice of law and venue

Any dispute or claim arising out of or in connection with this DPA shall be settled at the Courts and be governed by the laws set out in the Agreement.