ENTERPRISEDB CORPORATION – DATA PROTECTION ADDENDUM

This Data Protection Addendum including, its Schedules and Appendices (the "**DPA**") forms part of the EnterpriseDB Corporation ("**EDB**", "**we**", "**our**", "**us**") BigAnimal Terms (the "**Terms**") entered into between the party identified as the "Customer" therein ("**Customer**", "**you**", "**your**") and EDB (each a "**Party**" and together, the "**Parties**") and as updated from time to time between the Parties.

This DPA has been entered into by the Parties to reflect their agreement with regard to the processing of personal data under or in connection with the Terms. This DPA only applies to the extent you are a corporate customer; and (i) the personal data processed by us in the course of our provision of Services to you, is subject to the GDPR and/or the FADP; or (ii) we are processing personal information of California residents in the course of our provision of Services to you.

Customer enters into this DPA as at the date of acceptance by Customer of the DPA ("**Effective Date**"), on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "**Customer**" shall include Customer and Authorized Affiliates.

In the course of providing services to Customer pursuant to the Terms (the "**Services**"), EDB may process personal data of Customer and the Parties agree to comply with the following provisions with respect to any such processing.

HOW TO EXECUTE THIS DPA:

- This DPA consists of three parts: (i) the main body of the DPA, (ii) Schedule 1 which includes the Standard Contractual Clauses, and (iii) Schedule 2 which constitutes the CCPA Addendum.
- This DPA has been pre-signed on behalf of EDB.
- By continuing to use of the Services you are deemed to have accepted and be bound by, as applicable, the terms of this DPA, the Standard Contractual Clauses, and/or the CCPA Addendum, incorporated herein. At this point this DPA will become legally binding. For the avoidance of doubt, acceptance of the DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices, and the CCPA Addendum, as applicable.
- By using the Services you confirm you are duly authorized by the Customer entity you represent to execute this DPA.

DATA PROTECTION TERMS:

1. **DEFINITIONS; INTERPRETATION**

1.1 The following terms shall have the following meanings:

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws of the European Economic Area ("**EEA**"), Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Terms;

"**CCPA Addendum**" means the addendum attached as Schedule 2 hereto;

"**Data Protection Laws**" means any applicable data protection or privacy laws, rules and regulations. It shall include as applicable (a) the EU e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; (b) the GDPR, (c) the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications (EC Directive) Regulations 2003, (d) the Federal Act on Data Protection as amended from time to time ("**FADP**"); (e) the California Consumer Privacy Act ("**CCPA**"), and (f) other laws, rules and regulations that are similar, equivalent to, or successors to the laws that are identified in (a) through (e) above;

"**EEA Restricted Transfer**" means a transfer of personal data from or which originated in the EEA to a Third Country that is not considered to provide an "adequate level" of data protection by the European Commission and where such transfer is subject to the EU GDPR;

"**GDPR**" means the EU General Data Protection Regulation 2016/679 ("**EU GDPR**") as implemented by countries within the EEA and the EU GDPR as retained as UK law by the European Union (Withdrawal) Act 2018 ("**UK GDPR**") (as applicable to the processing);

"**Personal Information**" shall have the same meaning ascribed to it under the CCPA;

"**Restricted Transfer**" means either an EEA Restricted Transfer, a Swiss Restricted Transfer or a UK Restricted Transfer;

"**Standard Contractual Clauses**" means the Standard Contractual Clauses attached at Schedule 1 hereto;

"**Swiss Restricted Transfer**" means a transfer of personal data from or which originated in Switzerland to a Third Country that is not considered to provide an "adequate level" of data protection by the Federal Data Protection and Information Commissioner ("**FDPIC**");

"**Third Country**" means a country outside of the EEA, Switzerland and the UK;

"**UK Restricted Transfer**" means a transfer of personal data from or which originated in the UK to a Third Country that is not considered to provide an "adequate level" of data protection by the UK Government and where such transfer is subject to the UK GDPR; and

The terms "**controller**", "**data subject**", "**personal data**" "**processor**", "**processing**", "**supervisory authority**" shall have the same meanings ascribed to them under the GDPR.

1.2 To the extent the terms contained in this DPA conflict with those contained in the Terms, the terms in this DPA shall prevail to the extent such conflict relates to the processing of personal data. To the extent the terms contained in this DPA conflict with those contained in Schedule 1 (Standard Contractual Clauses) or Schedule 2 (CCPA Addendum), the terms in Schedule 1 (Standard Contractual Clauses) and Schedule 2 (CCPA Addendum) shall respectively prevail to the extent of such conflict.

2. GENERAL

2.1 Each Party shall comply with Data Protection Laws and the terms of this DPA.

2.2 The Parties acknowledge that if a Customer ("**Data Exporter**") undertakes a Restricted Transfer of personal data to EDB ("**Data Importer**") the Parties shall process personal data which is subject to the Restricted Transfer ("**Transferred Data**") in accordance with the terms of clause 3 below and Schedule 1 hereto. The Parties further acknowledge that:

(a) if each of the Data Exporter and the Data Importer is a controller, Module 1 of the Standard Contractual Clauses applies to the processing; and

(b) if the Data Exporter is a controller and the Data Importer is a processor, Module 2 of the Standard Contractual Clauses applies to the processing.

2.3 The Parties acknowledge that if EDB processes personal information of California residents, the terms of Schedule 2 hereto shall apply.

3. **RESTRICTED TRANSFERS**

3.1 Where the Data Exporter carries out a UK Restricted Transfer, the Standard Contractual Clauses shall be deemed amended as follows:

(a) all references to "*Regulation (EU) 2016/679*" or "*that Regulation*", shall be read as "*Regulation (EU) 2016/679 as retained as UK law by the European Union (Withdrawal) Act 2018*";

(b) all references to specific Article(s) of "*Regulation (EU) 2016/679"* are replaced with the equivalent Article of the UK GDPR;

(c) all references to "*Regulation (EU) 2018/1725"* are removed;

(d) Clause 13(a) and Part C of Annex II are not used and the competent supervisory authority for purposes of Clause 13 of the Standard Contractual Clauses shall be the UK's Information Commissioner's Office;

(e) the governing law shall be that of England & Wales for purposes of Clause 17 of the Standard Contractual Clauses;

(f) all references to "*Union*", "*EU*", and "*EU Member State*" are to be replaced with "*UK*";

(g) Clause 18 is replaced to state "*Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.";* and

(h) the footnotes to the Clauses shall not apply.

3.2 Where the Data Exporter carries out a Swiss Restricted Transfer, the Standard Contractual Clauses shall be deemed amended as follows:

(a) the term "personal data" shall be deemed to include information relating to an identified or identifiable legal entity. The list of data subjects and categories of data indicated in Annex I(B) to the Standard Contractual Clauses shall not be deemed to

restrict the application of the Standard Contractual Clauses to personal data which is subject to this clause 3.2;

(b) references to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the FADP;

(c) reference to the competent supervisory authority in Annex I(C) under Clause 13 shall be deemed to refer to the FDPIC;

(d) references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland;

(e) references to the exporter in the EU shall be deemed to include the exporter in Switzerland;

(f) references to the European Union in Clause 8.8 of Module 2 and in Annex I (A) shall be deemed to include Switzerland; and

(g) where the Clauses use terms that are defined in the EU General Data Protection Regulation 2016/679, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP.

3.3 Where the Restricted Transfer is made pursuant to Module 2 of the Standard Contractual Clauses, the Data Importer shall, taking into account the nature of processing and the information available to the Data Importer, provide assistance to the Data Exporter to enable the Data Exporter to carry out data protection impact assessments in relation to the Transferred Data. The Data Exporter agrees to consult with the supervisory authority prior to processing where a data protection impact assessment indicates that the processing of Transferred Data would result in a high risk to relevant data subjects.

3.4 Where the Restricted Transfer is made pursuant to Module 1 of the Standard Contractual Clauses, the Data Importer shall, shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations set out in the Standard Contractual Clauses and at the Data Exporter's request, allow for and contribute to audits of the processing activities covered by the Standard Contractual Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the Data Exporter may take into account relevant certifications held by the Data Importer. The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Sponsor and shall, where appropriate, be carried out with reasonable notice.

3.5 Where the Data Exporter carries out a Restricted Transfer it shall ensure that Transferred Data is accurate and limited to what is necessary for the receipt of services from the Data Importer.

3.6 Where Data Importer receives a valid and binding order from any governmental body ("**Requesting Party**") for a disclosure of Transferred Data, Data Importer will use every reasonable effort to redirect the Requesting Party to request Transferred Data directly from Data Exporter.

3.7 For the purposes of clause 8.5(a) of Module 1 and clause 8.6(a) of Module 2, Data Exporter is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in Annex II of the Standard Contractual Clauses meet Data Exporter's requirements and agrees that (taking into account the state of the art, the costs of

implementation, and the nature, scope, context and purposes of the processing of Transferred Data as well as the risks to data subjects) the security measures and policies implemented and maintained by Data Importer provide a level of security appropriate to the risk with respect to its Transferred Data.

4. **DATA SUBJECTS AND ENFORCEMENT**

4.1 Except to the extent set out in clause 4.2, it is the express intent of the Parties that any person who is not a party to this DPA has no right, as third party beneficiary, under local legal principle or law, to enforce any term of this DPA, and accordingly nothing contained in this DPA will entitle any person (including, data subjects) other than the parties to this DPA, to any claim, cause of action, remedy or right of any kind whatsoever.

4.2 Notwithstanding the provisions of clause 4.1 above, the Parties agree that a data subject may enforce the terms of the Standard Contractual Clauses as provided therein and the Parties acknowledge that nothing in this DPA restricts data subjects from exercising their rights under Data Protections Laws, including their rights to compensation from Data Importer for material or non-material damage.

5. **TERM AND TERMINATION**

5.1 This DPA enters into force as of the Effective Date for an indefinite term unless and until terminated as stated herein below.

5.2 Subject at all times to the termination provisions in the Standard Contractual Clauses, in the event that:

(a) Data Importer gives notice to Data Exporter that it is unable to comply with its obligations under Data Protection Laws, the Standard Contractual Clauses or the CCPA Addendum; or

(b) Data Importer is in material breach of any of its obligations under this DPA (including, the Standard Contractual Clauses or the CCPA Addendum) and such breach is incapable of being remedied or has not been remedied within 90 days of receipt of written notice to cure from any party; or

(c) a supervisory authority, or a tribunal or court rules that there has been a breach of any relevant laws in its jurisdiction by virtue of a Data Importer's processing of personal data under or in connection with this DPA,

the Data Exporter, without prejudice to any other rights that it may have against the Data Importer, shall be entitled to:

(d) require the Data Importer to cease its processing of the personal data; or

(e) terminate this DPA.

5.3 In the event that Data Exporter is in material breach of any of its obligations under this DPA and such breach is incapable of being remedied or has not been remedied within 90 days of receipt of written notice to cure from any party, the Data Importer, without prejudice to any other rights that it may have against the Data Exporter, shall be entitled to:

(a) cease its processing of the relevant personal data; or

(b) terminate this DPA.

5.4 Notwithstanding anything else in this clause 5 or the Standard Contractual Clauses, the parties agree that the termination of this DPA at any time, in respect of any party in any circumstances and for whatever reason, does not exempt the relevant terminated party from the obligations and/or conditions under this DPA as regards the processing of personal data.

6. AMENDMENTS

6.1 EDB shall notify the Customer of any proposed amendment to this DPA. Each proposed amendment to this DPA shall be deemed accepted by the Customer and this DPA shall be deemed so amended 30 days from the date such notification is sent to the Customer. If the Customer signifies its non-acceptance of such proposed amendment within said 30-day period EDB shall promptly commence discussions with the Customer in order to reach an outcome satisfactory to all Parties.

6.2 Notwithstanding the foregoing, the Parties acknowledge that should the UK Government publish new standard contractual clauses (or amendments to the existing standard contractual clauses) to address UK Restricted Transfers, such new standard contractual clauses will be automatically incorporated into this DPA where EDB provides notice of this to the Customer and all UK Restricted Transfers will be thereafter made pursuant to such new or amended standard contractual clauses.

7. MISCELLANEOUS

7.1 Failure by any party to enforce any of its rights under this DPA shall not be taken as or deemed to be a waiver of such right.

7.2 If any part, term or provision under this DPA is held to be illegal or unenforceable, the validity or enforceability of the remainder of this DPA will not be affected.

7.3 This DPA shall be interpreted according to and governed by the laws of the Commonwealth of Massachusetts, without regard to the conflicts of law provisions therein, except for those provisions or clauses that dictate the application of another law. Each Party irrevocably agrees that the courts of Middlesex County, Massachusetts shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA or its subject matter or formation. Notwithstanding the foregoing, the provisions set out in Schedule 1 of this DPA shall be governed by, and subject to the jurisdiction of, the relevant law and courts as set forth in Schedule 1.

IN WITNESS WHEREOF, the parties hereto have caused this DPA to be executed as of the Effective Date.

SIGNED by Paul R. Lucchese for and on behalf of **EnterpriseDB Corporation**	)	Signature:
	)	Position:

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);;

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 Optional

Docking clause - *Intentionally left blank.*

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE ONE: Transfer controller to controller

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(a) where it has obtained the data subject's prior consent;

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

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

8.2 **Transparency**

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or

providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 **Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

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

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

8.4 **Storage limitation**

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

8.5 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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

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

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

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

8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country,

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation,

hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(a) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(c) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(e) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

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

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

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

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

8.9 **Documentation and compliance**

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

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

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

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

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data,

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

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

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

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

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

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

8.9 **Documentation and compliance**

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

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

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

MODULE TWO: Transfer controller to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[5] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[6] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

---

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

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

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

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

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

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

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

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

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

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

MODULE TWO: Transfer controller to processor

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational

measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(i) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

Clause 13

Supervision

(a) **Where the data exporter is established in an EU Member State**: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be

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

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

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 **Notification**

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

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall

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

include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

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

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

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Netherlands.

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

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

APPENDIX

ANNEX I(1) – MODULE 1 TRANSFERS

This Annex includes Restricted Transfers which fall within scope of Module 1 only.

A. LIST OF PARTIES

Data exporter(s):

Name: Details as provided in Customer's EDB account.

Address: Details as provided in Customer's EDB account.

Contact person's name, position and contact details: Details as provided in Customer's EDB account.

Activities relevant to the data transferred under these Clauses: Customer account management purposes in connection with the provision of Services by data importer to data exporter.

Signature and date: Through continued use of the Services under the Terms, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: EnterpriseDB Corporation

Address: 34 Crosby Drive, Suite 201, Bedford, MA 01730 (USA)

Contact person's name, position and contact details: Details as provided in the Terms

Activities relevant to the data transferred under these Clauses: Customer account management purposes in connection with the provision of Services by data importer to data exporter.

Signature and date:

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Data exporter personnel,

Categories of personal data transferred

- Name
- Username
- Email address

- Telephone number

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None, except if data exporter chooses to transfer sensitive personal data.

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

One-off

Nature of the processing

Personal data will be subject to automated and manual processing operations including, collection, use, analysis, transfer, storage and erasure.

Purpose(s) of the data transfer and further processing

- To provide the Services under the Terms including, e.g., account creation and management

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For as long as necessary to fulfil the purposes for which it was transferred, including for the purposes of satisfying any legal, accounting or reporting requirements. To determine the appropriate retention period, the amount, nature and sensitivity of the personal data are considered, together with the necessity and purposes for the processing (including, whether such purposes can be achieved through other means) and the potential risk of harm from unauthorized use or disclosure of the personal data.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Deliberately left blank

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

Pursuant to Clause 13, the supervisory authority of the EEA country where (i) the data exporter is established; or where (ii) the EU representative of the data exporter is established; or where (iii) the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

ANNEX I(2) – MODULE 2 TRANSFERS

This Annex includes Restricted Transfers which fall within scope of Module 2 only.

A. LIST OF PARTIES

Data exporter(s):

Name: Details as provided in Customer's EDB account.

Address: Details as provided in Customer's EDB account.

Contact person's name, position and contact details: Details as provided in Customer's EDB account.

Activities relevant to the data transferred under these Clauses: Provision of Services by data importer to data exporter.

Signature and date: Through continued use of the Services under the Terms, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: EnterpriseDB Corporation

Address: 34 Crosby Drive, Suite 201, Bedford, MA 01730

Contact person's name, position and contact details: Details as provided in the Terms

Activities relevant to the data transferred under these Clauses: Provision of Services by data importer to data exporter.

Signature and date:

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Individuals whose personal data are collected and processed by data exporter – including, for example, data exporter personnel, clients, end-users, vendors.

Categories of personal data transferred

- Personal data included in content or data provided by or on behalf of Customer via the Services

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training),

keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- None

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

Continuous.

Nature of the processing

Personal data will be subject to automated and manual processing operations including, collection, use, analysis, transfer, storage and erasure.

Purpose(s) of the data transfer and further processing

- Provision of Services to the data exporter by the data importer

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the data exporter's subscription period and thereafter deleted or returned to the customer unless otherwise agreed and instructed by the customer.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Deliberately left blank

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Pursuant to Clause 13, the supervisory authority of the EEA country where (i) the data exporter is established; or where (ii) the EU representative of the data exporter is established; or where (iii) the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex describes data importer's security measures. Data exporter acknowledges that the Service operates pursuant to a shared responsibility model, which requires, among other things, that data exporter take certain steps such as protecting the security of data exporter data (which remains stored within data exporter's environment under data exporter's control). If and to the extent that data importer processes data exporter personal data on behalf of data exporter in connection with the Service, data exporter shall implement the following measures.

The data importer has implemented the following technical and organisational measures to ensure a level of security in line with the nature, scope, context, and purpose of the processing and the risks the processing presents for the rights and freedoms of natural persons:

Measures of pseudonymisation and encryption of personal data*: Encryption is enabled for data stores housing sensitive data. Company-issued laptop hard drives are encrypted using full disk encryption.*

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*: Data importer has in place a vulnerability monitoring and management policy which remediates vulnerabilities based on prescribed timelines. All employees complete training courses covering basic information security practices upon hire and annual thereafter. Data importer conducts a SOC 2 Type 1 Report on at least an annual basis and annual third-party cybersecurity audits.*

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*: For Module 2 transfers only: data importer shall take reasonable measures to ensure that personal data is protected against accidental destruction or loss. Data importer has implemented a secure backup system infrastructure to provide backup, retention, and restoration of data in the production environment. The data importer also has a business continuity program (BCP) and a disaster recovery plan (DRP) which are tested annually.*

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*: An internal risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. Data importer also conducts annual third-party audits.*

Measures for user identification and authorisation*: Data importer shall take reasonable measures to provide that any personal data is accessible and manageable only by properly authorized staff. Direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to personal data to which they have access privileges and that personal data cannot be read, copied, modified or removed without authorization in the course of processing.*

Input control - *data importer shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed.*

System access controls *– data importer shall take reasonable measures to prevent unauthorized use of the systems used for processing personal data. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, strong authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.*

Logical separation - *personal data in data importer's control is logically segregated on systems managed by the data importer to prevent unauthorized access.*

Measures for the protection of data during transmission and during storage*: Personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport. Data importer uses industry standard firewall and encryption technologies to protect data in transit and at rest. Any transfer of personal data to a third-party service provider is made via a secure transmission.*

Measures for ensuring physical security of locations at which personal data are processed*: The physical security and information security standards for Microsoft Azure's data centers are detailed at:* **https://docs.microsoft.com/en-us/azure/security/**.

Measures for ensuring events logging*: The data importer has implemented agent-based monitoring infrastructure or custom script-based monitoring within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potential unauthorized activity and security events. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events, and sending the aggregated abnormal log information to a centralized log repository either at regular intervals or in real time.*

Measures for ensuring system configuration, including default configuration *: The data importer has in place a password policy which requires an 8-character minimum and complexity enabled. Remote access to production systems is restricted to authorized employees with valid multi-factor authentication (MFA) tokens.*

Measures for internal IT and IT security governance and management*: The Data Importer has an Executive Management team that meets semi-annually with operational management to assess the effectiveness and performance of internal controls within the environment.*

Measures for ensuring data minimisation*: Data importer has in place policies and procedures to ensure that personal data processing is adequate, relevant and limited to what is necessary.*

Measures for ensuring limited data retention *: . Formal data retention and disposal procedures are documented to guide the secure retention and disposal of personal data, including a Data Classification Policy.*

Measures for ensuring accountability*: Data importer maintains an Article 30 GDPR record of processing.*

Measures for allowing data portability and ensuring erasure*: Data importer has in place a process for handling data subject rights' requests.*

Measures for handling and responding to data subject rights' requests*: Data importer has in place a process for handling data subject rights' requests.*

ANNEX III – LIST OF SUB-PROCESSORS

[*Deliberately left blank*]

SCHEDULE 2

CALIFORNIA CONSUMER PRIVACY ACT ADDENDUM

This CCPA Addendum specifies certain data protection obligations of EDB when processing the personal information of California residents in accordance with the California Consumer Privacy Act ("**CCPA**").

1. **Data Use**.

EDB shall process personal information of California residents only as necessary for the purposes of performing the Services. EDB shall not retain, use, or disclose the personal information of California residents obtained in the course of providing the Services except:

(a) To process or maintain the personal information of California residents on behalf of the Customer, and in compliance with the Terms;

(b) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements of a subcontractor under the CCPA and implementing regulations. If EDB discloses the personal information of California residents to a subcontractor for such purposes, EDB must execute a written agreement with the subcontractor obligating them to abide by the same restrictions regarding the retention, use or disclosure of California residents' personal information as are set forth in this CCPA Addendum;

(c) For internal use to build or improve the quality of its services, provided that the use does not include building or modifying profiles of California residents or households to use in providing services to another business, or correcting or augmenting data acquired from another source;

(d) To detect data security incidents or protect against fraudulent or illegal activity; or

(e) To comply with legal requirements, comply with a subpoena or similar legal process or government request, cooperate with law enforcement concerning conduct or activities that are reasonably and in good faith believed to violate applicable laws, or exercise or defend legal claims. EDB will notify Customer of such uses, unless doing so would, in EDB's good-faith belief, violate applicable law or directives from law enforcement or other governmental agencies.

2. **Data Subject Requests**.

(a) EDB shall not respond to any requests related to personal information processed on behalf of Customer other than to inform the requestor that EDB is not authorized to directly respond to a request, and recommend the requestor submit the request directly to Customer.

(b) EDB agrees to provide reasonable assistance, at Customer's expense, to support Customer in fulfilling its obligations to respond to data subject requests for access, erasure, deletion, do not sell, and any other similar data subject requests mandated by applicable law.