COLLIBRA VENDOR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between either Collibra Inc., Collibra UK Limited, or Collibra Belgium BV, as applicable based on the contracting entity identified in the Agreement ("**Collibra**"), and the vendor, as identified in the Agreement ("**Vendor**"), and amends and forms part of the agreement between Collibra and Vendor for Vendor's provision of services to Collibra (the "**Agreement**"). This DPA is made effective as of the date of the Agreement and prevails over any conflicting term of the Agreement (except with respect to the Agreement's liability and indemnification provisions), but does not otherwise modify the Agreement. Collibra may modify this DPA from time to time, provided that any material notifications shall take effect only after thirty (30) days' written notification to Vendor.

1. **Scope and Purpose of DPA**

1.1. This DPA applies to processing of personal data provided by Collibra to Vendor for the purposes of (a) providing the services under the Agreement (the "**Services**"), and (b) maintaining, processing or otherwise managing such data for the benefit of and on the behalf of Collibra and under the exclusive direction and control of Collibra, in each case in Vendor's capacity as a service provider of Customer ("**Covered Data**"). All other processing of personal data provided by Collibra to Vendor shall be clearly specified and agreed to by Collibra in the Agreement.

1.2. Vendor shall process Covered Data in compliance with applicable laws, rules and regulations. The Schedules to this DPA address compliance with specific jurisdictional privacy laws, rules and regulations, and only govern Vendor's processing of Covered Data hereunder to the extent such privacy laws, rules or regulations have jurisdiction over such Covered Data or Vendor's processing thereof.

1.3. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. **Personnel**

2.1. Vendor must implement appropriate technical and organizational measures to ensure that natural persons acting under the authority of Vendor ("**Personnel**") do not process Covered Data except on the instructions of Collibra.

2.2. Vendor must ensure that all Personnel authorized to process Covered Data are subject to a contractual or statutory obligation of confidentiality.

2.3. Vendor must regularly train Personnel regarding the protection of Covered Data.

2.4. Before assigning any individual to perform services or other obligations under the Agreement, Vendor shall conduct (and shall cause its approved subcontractors to conduct) a background check that satisfies a) industry standard general background check requirements, including (i) the previous three (3) years of employment, (ii) an address history trace for the last seven (7) years, (iii) professional credentials verification and (iv) credit history, and b) industry standard criminal background check requirements, including (i) local, regional, national or other territorial criminal history, including violent and economic criminal history, based upon the addresses revealed by the address history trace, (ii) sexual offender or similar sexual misconduct registries, (iii) global terror reports and (iv) an OFAC check.

3. **Security and Personal Data Breaches**

3.1. Vendor must implement technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing of Covered Data, including, as appropriate:

a) encryption and pseudonymization of Covered Data;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing;

c) measures to detect breaches of Covered Data in a timely manner;

d) measures to restore the availability and access to Covered Data in a timely manner in the event of an incident;

e) processes for regularly testing, assessing and evaluating the effectiveness of the security measures; and

f) without limiting the foregoing, the measures listed in Appendix 1 to this DPA.

3.2. Vendor must inform Collibra promptly and no later than forty-eight (48) hours after becoming aware of a breach involving Covered Data. Vendor must, either in the initial notice or in subsequent notices as soon as the information becomes available, inform Collibra of the nature of the Covered Data breach, the categories and number of individual persons affected, the categories and amount of Covered Data, the likely consequences of the Covered Data breach, and the measures taken or proposed to be taken to address the breach and mitigate possible adverse effects. If Vendor's notice or subsequent notices are delayed, they must be accompanied by reasons for the delay.

3.3. Vendor must document all Covered Data breaches, including at least the information referred to in Section 3.2, and provide a copy to Collibra upon request.

4. Audit

4.1. Vendor must make available to Collibra all information necessary to demonstrate compliance with the obligations of applicable privacy laws and this DPA and allow for and contribute to audits, including inspections, conducted by an applicable, authorized governmental regulatory authority, Collibra or another auditor mandated by Collibra.

4.2. Collibra and Vendor each bear their own costs related to an audit. If an audit determines that the Vendor violated any applicable privacy law or this DPA, then Vendor shall bear all costs related to the audit.

5. Liability

5.1. Vendor is fully liable to Collibra for any applicable data privacy laws or this DPA by Vendor or Vendor's Processors.

5.2. Where Collibra has paid damages or fines, Collibra is entitled to claim back from Vendor that part of the compensation, damages or fines, corresponding to Vendor's part of responsibility for the damages or fines.

5.3. Vendor must indemnify Collibra, its affiliates, directors, officers and personnel against all claims by third parties and resulting liabilities, losses, damages, costs and expenses (including reasonable external legal costs, administrative fines and other penalties) suffered or incurred by any of them, whether in contract, tort (including negligence) or otherwise arising out of or in connection with any infringement by Vendor or Vendor's subcontractors of this DPA or its obligations under applicable data privacy laws.

6. Confidentiality

6.1. Vendor must keep all Covered Data and all information relating to the processing thereof, in strict confidence.

6.2. Vendor authorizes Collibra to disclose the name(s) of Vendor and Vendor's subcontractors processing Covered Data, including by publishing a list on Collibra's website.

7. Notifications

7.1. Vendor must make all notifications required under this DPA at least to Collibra's Data Protection Officer via email to privacy@collibra.com.

7.2. Vendor must make all notifications relating to the security of processing to the contact identified in **Section 7.1** and to Collibra's Chief Information Security Officer via email to security@collibra.com.

8. Term and duration of Processing

8.1. Vendor's processing of Covered Data will last no longer than the term of Agreement and for a period of up to ninety (90) days thereafter solely for as long as is necessary to delete such Covered Data in accordance with Vendor's data retention practices.

8.2. Upon termination of the processing of Covered Data, Vendor must delete all Covered Data from within ninety (90) days after confirmation of Collibra's choice.

8.3. This DPA is terminated upon Vendor's deletion of all remaining copies of Covered Data in accordance with **Section 8.2**.

9. Modification of this DPA

This DPA may only be modified by a written amendment signed by both Collibra and Vendor.

10. Invalidity and severability

If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Schedule 1

European Data Protection Law

This Schedule 1 to the DPA applies to the processing of Covered Data under European Data Protection Law, as defined herein.

1. Definitions

In this DPA:

1.1. "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory** Authority" have the meaning given to them in European Data Protection Law;

1.2. "**European Data Protection Law**" means Data Protection Directive 95/46/EC, General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), and their national implementations in the European Economic Area ("EEA") and Switzerland, and the UK General Data Protection Regulation, each as applicable, and as may be amended or replaced from time to time;

1.3. "**Data Subject Rights**" means all rights granted to Data Subjects by European Data Protection Law, including the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

1.4. **Europe**" or "**European**" means the European Union, the European Economic Area, Switzerland, and the United Kingdom, including their respective member states and constituent states;

1.5. "**International Data Transfer**" means any transfer of Personal Data from Europe to an international organization or to a country outside of Europe, and includes any onward transfer of Personal Data from the international organization or the country outside of Europe to another international organization or to another country outside of Europe;

1.6. "**Sensitive Data**" means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under European Data Protection Law or other laws to which Collibra is subject;

1.7. "**Standard Contractual Clauses**" means (a) the clauses annexed to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972, and (b) solely to the extent applicable, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as promulgated under the UK GDPR.

1.8. "**Subprocessor**" means a Processor engaged by Vendor to carry out Processing on behalf of Collibra.

2. Roles and Scope

2.1. Collibra is a Controller and appoints Vendor as a Processor on behalf of Collibra.

2.2. This Schedule 1 applies to all Processing of Personal Data by Vendor as a Processor in the context of the Agreement. This Schedule 1 shall not apply to Personal Data Processing by Vendor as a Controller.

2.3. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in **Attachment 2 to this Schedule 1**, which is an integral part of **this Schedule 1**.

3. Instructions

3.1. Vendor must only Process Personal Data in compliance with the European Data Protection Law, including, but not limited, to the following:

a) Vendor must only Process Personal Data on documented instructions of Collibra, and is prohibited from Processing Personal Data for any other purpose; and

b) Collibra's instructions are documented in **Attachment 2 to** this **Schedule 1**, the Agreement, and any applicable statement of work.

3.2. Collibra may issue additional instructions to Vendor as it deems necessary to comply with European Data Protection Law.

4. Subprocessing

4.1. Vendor must obtain Collibra's prior authorization to engage Subprocessors. Collibra hereby authorizes Vendor to engage the Subprocessors referenced on **Attachment 1 to this Schedule 1**. In the event Vendor desires to add a new Subprocessor, Vendor shall notify Collibra's Data Protection Officer in writing at least thirty (30) days in advance via privacy@collibra.com. Collibra shall have the right to terminate the Agreement and the processing of Covered Data upon notice to Vendor in the event Collibra objects to the engagement of such Subprocessor.

4.2. Vendor must obtain sufficient guarantees from all Subprocessors that they will implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of European Data Protection Law and this DPA.

4.3. Vendor must enter into a written agreement with all Subprocessors which imposes the same obligations on the Subprocessors as this DPA imposes on Vendor.

4.4. Vendor must provide a copy of Vendor's agreements with Subprocessors to Collibra upon request. Vendor may redact commercially sensitive information before providing such agreements to Collibra.

4.5. If any Subprocessor fails to fulfil its obligations under European Data Protection Law, this DPA, or the agreements between Vendor and Subprocessor, Vendor will be fully liable to Collibra for the performance of such obligations.

5. International Data Transfers

5.1. Vendor must obtain Collibra's prior written authorization to perform International Data Transfers. Collibra hereby authorizes Vendor to perform International Data Transfers on the basis of a valid adequacy decision of the EU Commission or appropriate safeguards in accordance with European Data Protection Law.

5.2. To the extent required. By European Data Protection Law, Vendor and Collibra NV, on behalf of itself and its Affiliates referenced here, hereby conclude the Standard Contractual Clauses attached as **Attachment** 3 to this Schedule 1.

5.3. Vendor must inform Collibra at least thirty (30) days prior to any intended change of International Data Transfers, including the country, and the legal basis of the International Data Transfer pursuant to **Section 5.1**.

5.4. All authorizations of International Data Transfers in **Section 5** are expressly conditioned upon Vendor's ongoing compliance with the requirements of European Data Protection Law applicable to International Data Transfers, and any applicable legal instrument for International Data Transfers. If such compliance is affected by circumstances outside of Vendor's control, including circumstances affecting the validity of an applicable legal instrument, Collibra and Vendor will work together in good faith to reasonably resolve such non-compliance.

6. Assistance

6.1. Vendor must assist Collibra, including by implementing appropriate technical and organizational measures, with the fulfilment of Collibra's own obligations under European Data Protection Law, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects;

c) replying to investigations and inquiries from Supervisory Authorities;

d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and

e) notifying Personal Data Breaches.

6.2. Unless prohibited by European law, Vendor must inform Collibra without undue delay if Vendor:

a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires Vendor to Process Personal Data in contravention of Collibra's instructions; or

d) is otherwise unable to comply with European Data Protection Law or this DPA.

6.3. Unless prohibited by European law, Vendor must obtain Collibra's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in **Section 6.2**.

7. Accountability

7.1. Vendor warrants that it possesses the expert knowledge, reliability and resources, and has implemented appropriate technical and organizational measures to meet the requirements of European Data Protection Law, including for the security of Processing.

7.2. Vendor must maintain records of all Processing of Personal Data, including at a minimum the categories of information required under European Data Protection Law, and must provide a copy of such records to Collibra upon request.

7.3. Vendor must inform Collibra without undue delay if Vendor believes that an instruction of Collibra violates European Data Protection Law, in which case Vendor may suspend the Processing until Collibra has modified or confirmed the lawfulness of the instructions in writing.

ATTACHMENT 1 TO SCHEDULE 1
SUBPROCESSORS

As attached to the Agreement.

Attachment 2 to Schedule 1
Description of the Processing

As attached to the Agreement.

Appendix 3 to Schedule 1

Standard Contractual Clauses (Controller to Processor and Processor to Processor)

Reading Guide:

*With respect to the implementation of the Standard Contractual Clauses under the Agreement, either one or both of Module Two: Controller to Processor of the Standard Contractual Clauses ("**Module Two**") and Module Three: Processor to Processor of the Standard Contractual Clauses ("**Module Three**") shall apply, and both Module Two and Module Three are referenced herein. To the extent Module Two and Module Three differ, those differences are highlighted below. Where Module Two and Module Three do not differ, the identical provisions are referenced only once.*

As specified in the Standard Contractual Clauses below, for both Module Two and Module Three, the following optional provisions are selected:

1. *Clause 7: Docking Clause*
2. *Clause 9(a) Use of Sub-processors: Option 2 General Written Authorization, with a notice period of 30 days has been selected.*
3. *Clause 11 Redress: The optional clause is not included.*
4. *Clause 17 Governing Law: Option 1, the governing law of Belgium.*
5. *Clause 18(b) Choice of Forum and Jurisdiction, the courts of Belgium.*

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) 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 add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(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) For Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); For Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

(iv) 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

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I. A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

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.

FOR 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 (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, or if:

(i) 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;

(ii) 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;

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

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

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

8.9 Documentation and compliance

(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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(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, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

(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 its controller so that the latter may in turn 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 set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 or if:

(i) 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;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

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

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

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

8.9 Documentation and compliance

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

(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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

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

(f) 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.

(g) 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

FOR 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 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. 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 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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(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

FOR 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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under

Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by 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;

(ii) 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

(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;

(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 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 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 Belgium.

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 Belgium.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

(1) Name: Collibra Belgium BV, on behalf of itself and its Affiliates as referenced here.

Address: Picardstraat 11 B 205, 1000, Brussels - Belgium

Contact person's name, position and contact details: Amanda Weare, Data Protection Officer, privacy@collibra.com

Activities relevant to the data transferred under these Clauses: As specified in the Agreement.

Signature and date: As indicated via signature to or other form of execution of the Agreement by Collibra

Role (controller/processor): Controller and/or processor, as applicable

Data importer(s):

(1) Name: Vendor, as specified in the Agreement.

Address: Vendor's address as specified in the Agreement.

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: As specified in the Agreement

Signature and date: As indicated via signature to or other form of execution of the Agreement by Collibra

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects concerned as identified in *Attachment* 2 to Schedule 1 of the DPA

Categories of personal data transferred

The categories concerned as identified in *Attachment* 2 to Schedule 1 of the DPA

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.

The special categories of data as identified in *Attachment* 2 to Schedule 1 of the DPA.

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

Continuous

Nature of the processing

The nature of the processing as identified in *Attachment* 2 to Schedule 1 of the DPA.

Purpose(s) of the data transfer and further processing

The purpose of the processing as identified in *Attachment* 2 to Schedule 1 of the DPA.

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

The duration of the processing as identified in *Attachment* 2 to Schedule 1 of the DPA.

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

As identified in *Attachment 1* to Schedule 1 of the DPA for the limited purposes described therein

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: Belgian Data Protection Authority.

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The security measures identified in Appendix 1 to the DPA

ANNEX III – LIST OF SUB-PROCESSORS

Clause 9(a) Option 2 is applicable. Subprocessors are referenced in *Attachment* 1 to Schedule 1 of the DPA

Information Commissioner's Office

1.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date of the Approved EU SCCs to which this Addendum is attached.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Collibra UK Limited Trading name (if different): n/a Main address (if a company registered address): 200 Aldersgate, 7th Floor, London, EC1A 4HD Official registration number (if any) (company number or similar identifier): N/A	Full legal name: Vendor name as specified in the Agreement. Trading name (if different): n/a Main address (if a company registered address): As specified in the Agreement. Official registration number (if any) (company number or similar identifier): N/A

Key Contact	Full Name (optional): Amanda Weare Job Title: Data Protection Officer Contact details including email: privacy@collibra.com	Full Name (optional): As specified in Annex I of the EU SCCs. Job Title: As specified in Annex I of the EU SCCs. Contact details including email: As specified in Annex I of the EU SCCs.
Signature (if required for the purposes of Section 2)	Binding upon execution of the Approved EU SCCs (to which this Addendum is attached)	Binding upon execution of the Approved EU SCCs (to which this Addendum is attached)

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:
	Date: Same as Approved EU SCCs which this Addendum is appended to
	Reference (if any):
	Other identifier (if any):

(a)

Table 3: Appendix Information

“**Appendix Information”** means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I to the Approved EU SCCs to which this Addendum is attached.

Annex 1B: Description of Transfer: See Annex I to the Approved EU SCCs to which this Addendum is attached.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to the Approved EU SCCs to which this Addendum is attached.
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III to the Approved EU SCCs to which this Addendum is attached.

(b)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Schedule 2

CCPA

This Schedule 2 to the DPA applies solely to the processing of Covered Data under CCPA, as defined herein.

1. Definitions.

In this Schedule 2:

1.1. "**CCPA**" means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 to 1798.199) and its implementing regulations, as amended or superseded from time to time.

1.2. The capitalized terms used in this Schedule 2 and not otherwise defined in this Addendum shall have the definitions set forth in the CCPA.

2. Roles and Scope.

2.1. This Schedule 2 applies to the collection, retention, use, disclosure, and sale of Personal Information by Vendor to provide Services to Collibra pursuant to the Agreement or to perform a Business Purpose.

2.2. Collibra is a Business and appoints Vendor as a Service Provider to process information on behalf of Collibra. This Schedule 2 applies solely with respect to Vendor's processing of Personal Information as a Service Provider of Collibra. This Addendum shall not apply to Personal Information collected by Vendor as a Business.

3. Restrictions on Processing.

3.1. Vendor is prohibited from retaining, using, or disclosing the Personal Information provided by Collibra or which is collected on behalf of Collibra for any purpose other than for the specific purpose of performing the Services specified in the Agreement for Collibra, as set out in this Addendum, or as otherwise permitted by the CCPA.

3.2. Vendor shall not further collect, sell, or use the Personal Information except as necessary to perform the Business Purpose.

4. Use.

Vendor warrants that it will not use the Personal Information it receives from or collects on behalf of Collibra in violation of the restrictions set forth in the CCPA.

5. Notice

Collibra represents and warrants that it has provided notice that information is being used or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i).

6. Consumer Rights.

6.1. Vendor shall provide reasonable assistance to Collibra in facilitating compliance with Consumer rights requests.

6.2. Upon direction by Collibra, and in any event no later than 30 days after receipt of a request from

Collibra, Vendor shall promptly delete Personal Information. Vendor shall not be required to delete any Personal Information to comply with a Consumer's request directed by Collibra if it is necessary to maintain such information in accordance with Cal. Civ. Code 1798.105(d), in which case Vendor shall promptly inform Collibra of the exceptions relied upon under 1798.105(d) and Vendor shall not use the Personal Information retained for any other purpose than provided for by that exception.

7. Deidentified Information.

In the event that either Party shares Deidentified Information with the other Party, the receiving Party warrants that it: (i) has implemented technical safeguards that prohibit reidentification of the Consumer to whom the information may pertain; (ii) has implemented business processes that specifically prohibit reidentification of the information; (iii) has implemented business processes to prevent inadvertent release of Deidentified Information; and (iv) will make no attempt to reidentify the information.

8. Mergers, Sale, or other asset transfer.

In the event that either Party transfers to a Third Party the Personal Information of a Consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the Third Party assumes control of all or part of such Party to the Agreement, that information shall be used or shared consistently with applicable law. If a Third Party materially alters how it uses or shares the Personal Information of a Consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the Consumer in accordance with applicable law.

9. As required by law.

Notwithstanding any provision to the contrary of the Agreement or this Addendum, Vendor may cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate federal, state, or local law.

10. Sale of Information

The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this DPA.

11. Consumer Directed Disclosure

Collibra may share Personal Information with Vendor at a Consumer's direction or intentional interaction with Services provided by Vendor. In the event Collibra shares Personal Information with Vendor in such a manner, Vendor agrees not to sell the Personal Information, unless that disclosure would be consistent with the provisions of the CCPA.

Appendix 1 to the Data Processing Addendum

Vendor Security Measures

Vendor will, at a minimum, implement the following types of security measures:

1. **Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Covered Data are Processed, include:

☐ Establishing security areas, restriction of access paths;
☐ Establishing access authorizations for employees and third parties;
☐ Access control system (ID reader, magnetic card, chip card);
☐ Key management, card-keys procedures;
☐ Door locking (electric door openers etc.);
☐ Security staff, janitors;
☐ Surveillance facilities, video/CCTV monitor, alarm system; and
☐ Securing decentralized data processing equipment and personal computers.

2. **Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

☐ User identification and authentication procedures;
☐ ID/password security procedures (must have alphanumeric password complexity and special characters enforced, minimum length enforced at 12 characters, ability to enforce password changes to specific durations, password lockout should be able to be enforced);
☐ Automatic blocking (e.g. password or timeout);
☐ Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
☐ Creation of *one* master record per user, user-master data procedures per data processing environment; and
☐ Encryption of archived data media.

3. **Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Covered Data in accordance with their access rights, and that Covered Data cannot be read, copied, modified or deleted without authorization, include:

☐ Internal policies and procedures based on known industry standards like ISO27kx, SOC2 or others;
☐ Third party attestation reports, if applicable, such as ISO27001, SOC1/2, HIPAA, penetration tests results, or others;
☐ Control authorization schemes;
☐ Differentiated access rights (profiles, roles, transactions and objects);
☐ Monitoring and logging of accesses; and
☐ Disciplinary action against employees who access Covered Data without authorization.