Last Updated February 24, 2026

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between either Collibra Inc. or Collibra UK Limited (depending on the nature of your Agreement as defined below) ("**Collibra**"), and you, a customer of Collibra products and/or services ("**Customer**"), and amends and forms part of the commercial agreement between Customer and Collibra for Collibra products and/or services (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. If required by applicable law, Collibra may modify this DPA with respect to such requirements upon written notice to Customer via an email notification to the email address(es) registered by Customer here. All other modifications shall require the prior written consent of Customer and Collibra.

1. Scope and Purpose of DPA

1.1 This DPA applies to processing of personal data provided by Customer to Collibra for the purposes of (a) providing the services under the Agreement (the "**Services**"), and (b) maintaining, processing or otherwise managing such data solely for the benefit of and on behalf of Customer and under the exclusive direction and control of Customer, in each case solely in Collibra's capacity as a service provider of Customer (collectively, the "**Covered Data**"). All personal data provided by Customer to Collibra in connection with the Services and/or its business relationship with Collibra that is not Covered Data is collected, processed, used and/or shared by Collibra in compliance with its Privacy Policy.

1.2 A description of the Covered Data processed, as well as the nature and duration of such processing, is set forth on Exhibit A to this DPA. Collibra strives to 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 Collibra's processing of Covered Data hereunder to the extent such privacy laws, rules or regulations have jurisdiction over such Covered Data or Collibra's processing thereof.

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

2. Confidentiality, Security and Personal Data Breaches

2.1 Collibra will ensure that all personnel authorized to process Covered Data are subject to an obligation of confidentiality.

2.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Collibra will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in the Collibra Security Policy.

2.3 Customer acknowledges that the security measures in the Collibra Security Policy are appropriate in relation to the risks associated with Customer's intended processing, and will notify Collibra prior to any intended processing for which Collibra's security measures may not be appropriate.

2.4 Collibra will notify Customer without undue delay after becoming aware of a data breach involving Covered Data. If Collibra's notification is delayed, it will be accompanied by reasons for the delay.

3. Audit Rights

3.1 Collibra must make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by an applicable, authorized governmental regulatory authority, or reasonably requested by Customer and performed by an independent auditor as agreed upon by Customer and Collibra. Further, Collibra will provide Customer with all reasonably necessary information to enable Customer to conduct and document required data privacy, protection, and other related risk assessments.

3.2 Collibra will inform Customer if Collibra believes that Customer's instruction under Section 3.1 infringes or violates applicable law. Collibra may suspend the audit or inspection, or withhold requested information until Collibra has modified or confirmed the lawfulness of the instructions in writing.

3.3 Collibra and Customer each bear their own costs related to an audit.

4. **Subprocessors**.

Exhibit B to this DPA identifies the current third parties and Collibra affiliated entities ("**Subprocessors**") processing Covered Data as part of the Services, as well as the procedure and notification process for the adding new Subprocessors. Specific obligations with respect to Subprocessors required under applicable law are addressed within the jurisdiction specific Schedules to this DPA.

5. **Termination and return or deletion**

5.1 This DPA is terminated upon Collibra's deletion of all Covered Data.

5.2 Customer may request return of Covered Data up to thirty (30) days after termination of the Agreement. Unless required or permitted by applicable law, Collibra will securely delete all remaining copies of Covered Data no later than 120 days after termination of the Agreement.

6. **Notifications**

Customer will send all notifications, requests and instructions under this DPA to Collibra's Data Protection Officer via email to privacy@collibra.com.

7. **No Liability**

In no event shall Collibra be liable for any damages, fines, or costs arising from or related to the acts or omissions of Customer in relation to the subject matter of this DPA, including to the extent that the Agreement requires Collibra to collect, use, retain, disclose, or reidentify any Covered Data as directed by Customer.

8. **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.

EXHIBIT A

DESCRIPTION OF THE PROCESSING

1. **Data Subjects**

The Covered Data processed concerns the following categories of data subjects:

#	Category
1	Users of the Services
2	Data subjects whose data Customer submits to the Services.

2. **Categories of Covered Data**

The Covered Data processed concerns the following categories of data:

#	Category
1	Contact information and roles and titles of Users of the Services, Collibra account access credentials, IP addresses of Users, and information about Users' use of the Services;
2	Any additional data submitted by Customer to the Services, including personal data which may be included in metadata or underlying data sources referenced by Customers in the Services.

3. **Special categories data**

The Covered Data processed concern the following special/ sensitive categories of data:

#	Category
1	Customers may submit any form of personal data, including special or sensitive categories of personal data to the Services. Whether this occurs is not within Collibra's control and depends on the nature of Customers' use of the Services.

4. **Nature and Purpose of the Processing**

The Covered Data processed will be subject to the following basic processing activities:

#	Operation
1	Allowing User access, differentiating User access and control rights, identifying data stewards and other roles and responsibilities within the product, User notifications related to product usage, and similar processing activities necessary to allow Users full access to and use of the Services
2	Profiling Customer personal data for Customer as performed by Customer within the Services
3	Customer referencing Customer personal data within the Services

5. **Duration of the Processing**

The Covered Data will be processed for the duration of the performance of the Services and shall be deleted no later than 120 days after the termination of the Agreement

EXHIBIT B

SUBPROCESSORS

Collibra Subprocessors are listed here, as may be updated from time to time by Collibra. When Collibra intends to engage a new Subprocessor, Collibra will notify Customer of the engagement at least thirty (30) calendar days before any new Subprocessor Processes any Covered Data, except that if Collibra reasonably believes engaging a new Subprocessor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Covered Data or avoid material disruption to the Services, Collibra will give such notice as soon as reasonably practicable. If, within fifteen (15) calendar days after such notice, Customer notifies Collibra in writing that Customer objects to Collibra's appointment of a new Subprocessor based on reasonable data protection concerns, Collibra will discuss such concerns in good faith with Customer to see whether they can be resolved. If the parties are not able to mutually agree to a resolution of such concerns, Customer, as its sole and exclusive remedy, may terminate the Agreement and receive a pro-rated refund for pre-paid, unused fees.

Any Subprocessor notification provided to Customer by Collibra as contemplated by this Exhibit B may be given by updating the Subprocessor page here and via an email notification to the email address which Customer provides to Collibra here.

Schedule 1

European Economic Area and UK Data Protection Law

This Schedule 1 to the DPA applies solely to the processing of Covered Data under EEA/UK Data Protection Law, as defined herein.

1. **Definitions**

In this Schedule 1:

1.1. "**Collibra BCRs**" means Collibra's Binding Corporate Rules for Processors which are incorporated by reference to this DPA, and the most current version of which are on Collibra's website here.

1.2 "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the EEA/UK Data Protection Law.

1.3. "**Customer Personal Data**" means any Personal Data of Customer, the Processing of which is subject to EEA/UK Data Protection Law, for which Customer or Customer's customers are the Controller, and which is Processed by Collibra to provide the Services.

1.4. "**EEA/UK 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 ("**UK GDPR**"), each as applicable, and as may be amended or replaced from time to time.

1.5. "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making in accordance with EEA/UK Data Protection Law.

1.6. "**International Data Transfer**" means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom.

1.7. "**Subprocessor**" means a Processor engaged by Collibra to Process Customer Personal Data.

1.8. "**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.

2. **Scope and applicability**

2.1. This Schedule 1 applies solely with respect to Collibra's Processing of Personal Data as a Processor. This Schedule 1 shall not apply to Personal Data Processing by Collibra as a Controller.

2.2. The subject matter, nature and purpose of the Processing, duration of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in Exhibit A to the DPA.

2.3. Where Customer is a Controller, Customer appoints Collibra as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of EEA/UK Data Protection Law applicable to Controllers.

2.4. If Customer is a Processor on behalf of other Controller(s), then Customer: is the single point of contact for Collibra; must obtain all necessary authorizations from such other Controller(s); undertakes to issue all instructions and exercise all rights on behalf of such other Controller(s); and is responsible for compliance with the requirements of EEA/UK Data Protection Law applicable to Processors.

2.5. Customer acknowledges that Collibra may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product development, and compliance with law. Collibra is the Controller for such Processing and will Process such data in accordance with EEA/UK Data Protection Law.

3. **Instructions**

3.1. Collibra will Process Customer Personal Data to provide the Services and in accordance with Customer's documented instructions.

3.2. The Controller's instructions are documented in this DPA, the Agreement, and any applicable statement of work.

3.3. Customer may reasonably issue additional instructions as necessary to comply with EEA/UK Data Protection Law. Collibra may charge a reasonable fee to comply with any additional instructions.

3.4. Unless prohibited by applicable law, Collibra will inform Customer if Collibra is subject to a legal obligation that requires Collibra to Process Customer Personal Data in contravention of Customer's documented instructions.

4. **Subprocessing**

4.1. Customer hereby authorizes Collibra to engage the Subprocessors as referenced on Exhibit B to the DPA.

4.2. Collibra will enter into a written agreement with Subprocessors, which imposes the same obligations as required by EEA/UK Data Protection Law.

4.3. Customer agrees that Customer's authorization to engage the Subprocessors and Collibra's obligations under Section 4.2 satisfy the requirements of the Standard Contractual Clauses between Customer and Collibra under Clause 9(a), as applicable.

4.4. Collibra will be responsible and liable for the acts, omissions or defaults of its Subprocessors in the performance of obligations under this DPA as if they were Collibra's own acts, omissions or defaults, except as otherwise set forth in the Agreement or required by EEA/ UK Data Protection Law.

5. **Assistance**

5.1. Taking into account the nature of the Processing, and the information available to Collibra, Collibra will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under EEA/UK Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

5.2. Collibra will maintain records of Processing of Customer Personal Data in accordance with EEA/UK Data Protection Law.

5.3. Collibra may charge a reasonable fee for assistance under this Section 5. If Collibra is at fault, Collibra and Customer shall each bear their own costs related to assistance.

6. **International Data Transfers**

6.1. Customer hereby authorizes Collibra to perform International Data Transfers to any country deemed adequate by the EU Commission; on the basis of appropriate safeguards in accordance with EEA/UK Data Protection Law; pursuant to Collibra's BCRs; or, where the BCRs are not applicable, pursuant to the Standard Contractual Clauses referred to in Section 6.2.

6.2. Customer and Collibra Inc., on behalf of itself and its affiliates outside of the EEA referenced here, shall conclude the Standard Contractual Clauses, attached hereto as Appendix 1 to this Schedule 1.

6.3. If Collibra's compliance with EEA/UK Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Collibra's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and Collibra will work together in good faith to reasonably resolve such non-compliance.

7. **Information Security Incidents**

Customer agrees that the provisions of Section 2 of this DPA shall satisfy the requirements of the Standard Contractual Clauses between Customer and Collibra under Clause 8.6.

8. **Audit**

Customer agrees that the provisions of Section 3 of this DPA shall satisfy the parties' rights and obligations of the Standard Contractual Clauses between Customer and Collibra under Clause 8.9.

APPENDIX 1 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 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 benefiting 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

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: Customer name, as specified in the Agreement

Address: Customer address, as specified in the Agreement

Contact person's name, position and contact details: As provided by data exporter here

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 Customer

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

Data importer(s):

(1) Name: Collibra Inc., on behalf of itself and its Affiliates outside of the EEA as referenced here

Address: 61 Broadway, 31st Floor, New York, NY 10006, USA

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): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects concerned as identified in Exhibit A to the DPA

Categories of personal data transferred

The categories concerned as identified in Exhibit A to 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 Exhibit A to 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 Exhibit A to the DPA.

Purpose(s) of the data transfer and further processing

The purpose of the processing as identified in Exhibit A to 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 Exhibit A to the DPA.

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

As identified in Exhibit B to the DPA for the limited purposes described here

C. COMPETENT SUPERVISORY AUTHORITY

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

As provided by data exporter here.

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

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 the Collibra Security Policy

ANNEX III – LIST OF SUB-PROCESSORS

Clause 9(a) Option 2 is applicable. Subprocessors are here.

Information Commissioner's Office

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: Customer name, as specified in the Agreement. Trading name (if different): N/A Main address (if a company registered address): Customer address, as specified in the Agreement Official registration number (if any) (company number or similar identifier): N/A	Full legal name: Collibra Inc., on behalf of itself and its Affiliates outside of the EEA as referenced here. Trading name (if different): n/a Main address (if a company registered address): 61 Broadway, 31st Floor, New York, NY 10006, USA Official registration number (if any) (company number or similar identifier): N/A

Key Contact	Full Name (optional): As provided by data exporter here Job Title: As provided by data exporter here Contact details including email: As provided by data exporter here	Full Name (optional): Amanda Weare Job Title: Data Protection Officer Contact details including email: privacy@collibra.com
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):

(i)

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 organizational measures including technical and organizational 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.

(i)

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

United States Processing

This Schedule 2 to the DPA applies solely to the processing of Covered Data in the United States.

1. **Definitions.**

In this Schedule 2:

1.1. "**Applicable Data Protection Law**" shall mean all applicable United States laws and regulations governing the privacy and protection of personal information, including, where applicable, but not limited to, the California Consumer Privacy Act ("CCPA") and its amendments including the California Privacy Rights Act ("**CPRA**").

1.2. The capitalized terms used in this Schedule 2 and not otherwise defined in this DPA shall have the definitions set forth in Applicable Data Protection Law.

2. **Roles and Scope.**

2.1. This Schedule 2 applies to the collection, retention, use, disclosure, and sale of Covered Data provided by Customer or which is collected on behalf of Customer by Collibra to provide Services to Customer pursuant to the Agreement or to perform a Business Purpose identified in Section 3 below.

2.2. Customer is a Business or a Controller under Applicable Data Protection Law.

2.3. Collibra is a Service Provider or a Processor under Applicable Data Protection Law.

2.4. This Schedule 2 applies solely with respect to Collibra's processing of Covered Data as a Service Provider or Processor of Customer. This Schedule 2 shall not apply to personal information collected by Collibra as a Business or Controller.

3. **Processing.**

3.1. Collibra shall process Covered Data in compliance with Applicable Data Protection Law.

3.2. A description of the Covered Data processed as well as the nature and duration of such processing is more specifically described on Exhibit A to the DPA.

3.3. Customer shall have the right to take reasonable steps to ensure that Collibra processes Covered Data in a manner consistent with Customer's obligations under Applicable Data Protection Law by exercising Customer's audit rights in Section 3 of this DPA.

3.4. Customer shall have the right, upon reasonable notice to Collibra, to prevent Collibra's unauthorized processing of Covered Data.

3.5. Collibra is prohibited from retaining, using, or disclosing the Covered Data provided by Customer or which is collected on behalf of Customer outside of the direct business relationship with Customer and/or for any purpose other than for the specific purpose of performing the Services specified in the Agreement for Customer, and as set out in this DPA, provided that, in accordance with the Applicable Data Protection Law, Collibra may process Covered Data for the following Business Purposes, in each case to the extent necessary and proportionate to such purposes:

3.5.1. Helping to ensure the security and integrity of the Services;

3.5.2. Identifying and repairing errors that impair existing intended functionality;

3.5.3. Short-term, transient use, provided that the Covered Data is not disclosed to another third party and is not used to build a profile about a consumer;

3.5.4. Undertaking internal research for technological development and demonstration; and

3.5.5. Undertaking activities to verify or maintain the quality or safety of the Services for the purposes of improving, enhancing and upgrading such Services.

3.6. Collibra will not "sell" or "share" (as defined by the CCPA) Covered Data. Collibra shall not further collect or use (in each case as defined under Applicable Data Protection Law) the Covered Data except in connection with the performance of the Services or foregoing Business Purposes.

3.7. Collibra shall not combine the Covered Data with personal information that it receives from, or on behalf of, a third party or collects from consumers (as defined under Applicable Data Protection Law), except that Collibra may combine Covered Data to perform any Business Purpose as permitted by this Schedule 2, this DPA, the Agreement, or Applicable Data Protection Law.

3.8. Collibra shall promptly inform Customer if it is unable to meet its obligations under this Schedule 2, this DPA, or under Applicable Data Protection Law as it pertains to Covered Data.

4. **Subprocessors**.

Currently, Collibra leverages the Subprocessors referenced here to process Covered Data. The addition of new Subprocessors by Collibra is subject to the terms of Exhibit B to the DPA. Collibra will bind all Subprocessors to terms and conditions substantially similar to those contained in this DPA, including this Schedule 2.

5. **Notice & Consent.**

Customer represents and warrants that it has provided notice to Consumers that Covered Data is being used or shared consistent with Applicable Data Protection Law. Further, Customer shall obtain all necessary consents from Consumers consistent with Applicable Data Protection Law for Customer and Collibra to perform the Services.

6. **Consumer Rights.**

6.1. Collibra shall provide reasonable assistance to Customer in facilitating compliance with Consumer rights requests, including access, deletion, updates and similar requests as required under Applicable Data Protection Law. Collibra shall forward any such requests promptly to Customer upon receipt. Collibra may charge a reasonable fee to comply with any additional instructions required to effectuate Consumer rights requests.

6.2. Upon direction by Customer, and in any event no later than thirty (30) days after receipt of a request from Customer, Collibra shall promptly delete Covered Data as directed by Customer. Collibra shall not be required to delete any Covered Data to comply with a Consumer's request directed by Customer if it is necessary to maintain such information in accordance with Applicable Data Protection Law, in which case Collibra shall promptly inform Customer of the exceptions relied upon under Applicable Data Protection Law and Collibra shall not use the Covered Data 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: (a) has implemented technical safeguards that prohibit reidentification of the Consumer to whom the information may pertain; (b) has implemented business processes that specifically prohibit reidentification of the information; (c) has implemented business processes to prevent inadvertent release of Deidentified Information; and (d) 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 Covered Data 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 Covered Data 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 DPA, Collibra 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 Covered Data 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.

Schedule 3

This Schedule 3 to the DPA applies solely to the processing of Covered Data in the UAE, if applicable.

1. **United Arab Emirates: ADGM**.

1.1 **Definitions**.

1.1.1 "ADGM Data Protection Laws" includes the Abu Dhabi Global Market ("ADGM") Data Protection Regulations 2021 ("DPR 2021"), and any corresponding decrees, regulations, or guidance.

1.1.2 "ADGM SCCs" means the contractual clauses adopted by the Commissioner of Data Protection effective from 2021-08-14 relating to the transfer of Personal Data outside the ADGM pursuant to DPR 2021.

1.2 **Personal Data Breach**. In addition to those terms contained in Section 2.4 of the DPA, immediately upon providing notice of a Personal Data Breach, Collibra shall provide to Customer the name and contact details of the contact point where more information can be obtained, which is: the Data Protection Officer, email: privacy@collibra.com.

1.3 **Restricted Transfers**. With regard to any Restricted Transfer subject to ADGM Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

1.3.1. a valid adequacy decision adopted by the Commissioner of Data Protection on the basis of Article 41 of the DPR 2021;

1.3.2. the appropriate standard contractual clauses adopted by the Commissioner of Data Protection from time to time; or

1.3.3. any other lawful data transfer mechanism, as laid down in ADGM Data Protection Laws.

1.4 **Standard Contractual Clauses**.

1.4.1. The DPA hereby incorporates by reference the ADGM SCCs. The Parties are deemed to have accepted, executed, and signed the ADGM SCCs where necessary in their entirety (including the annexures thereto).

1.4.2. The Parties agree that any references to clauses, annexures, modules and choices within this Section 1.4 (Standard Contractual Clauses) shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated ADGM SCCs as may be applicable from time to time pursuant to the DPA.

1.4.3. For the purposes of the ADGM SCCs and any substantially similar standard contractual clauses which may be adopted by the relevant authorities in the future:

(A) the Parties agree to apply the following modules:

1) Module Two with respect to Controller-to-Processor Restricted Transfers; and

2) Module Three with respect to Processor-to-Sub-Processor Restricted Transfers.

(B) Clause 7: The Parties choose to include the optional docking clause;

(C) Clause 9(a): The Parties choose option 2, "General Written Authorization," and the time period, procedures for designation and notification of new Subprocessors are set forth in more detail in Exhibit B of the DPA;

(D) Clause 11: The Parties choose not to include the optional redress clause;

(E) Clause 17: The ADGM SCCs shall be governed by the laws of England and Wales;

(F) Clause 18: Any dispute arising from the ADGM SCCs shall be resolved by the competent courts of England;

(G) Annex I: The content of Annex I is set forth in Exhibit A of the DPA;

(H) Annex II: The content of Annex II is set forth in Section 2.2 of the DPA; and

(I) Annex III: The content of Annex III is set out in Exhibit B of the DPA.

1.4.4. In cases where the ADGM SCCs apply and there is a conflict between the terms of the DPA and the terms of the ADGM SCCs, the terms of the ADGM SCCs shall prevail with regard to the Transfer in question.

1.5 **General**. Collibra shall fully co-operate, on request, with the ADGM Office of Data Protection in the performance of Collibra's obligations under the ADGM Data Protection Laws.

2. **United Arab Emirates: DIFC**.

2.1 **Definitions**.

2.1.1. "Commissioner" means the DIFC Commissioner of Data Protection.

2.1.2. "DIFC Data Protection Laws" includes the Dubai International Financial Centre ("DIFC") Data Protection Law No. 5 of 2020, as amended by DIFC Law No. 2 of 2022 ("DP Law 2020"), the DIFC Data Protection Regulations of 2020 ("Regulations"), and any corresponding decrees, regulations, or guidance.

2.1.3. "DIFC SCCs" means the contractual clauses adopted by the Commissioner in accordance with regulations relating to the transfer of Personal Data outside the DIFC pursuant to DP Law 2020.

2.2 **Personal Data Breach**. In addition to those terms contained in Section 2.4 of the DPA, immediately upon receiving notice of a Personal Data Breach, Customer may contact Collibra's Data Protection Officer via email to privacy@collibra.com for more information thereon. Collibra shall fully co-operate with any investigation of the Commissioner in relation to a Personal Data Breach.

2.3 **Audit Rights**. In addition to those terms contained in Section 3 (Audit Rights) of the DPA, Collibra shall make available to the Commissioner, upon request, all information necessary to demonstrate compliance with the obligations laid down in this Section 2 (United Arab Emirates: DIFC) and the DPA, and allow for and contribute to audits, including inspections, conducted by the Commissioner.

2.4 **Restricted Transfers**. With regard to any Restricted Transfer subject to DIFC Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

2.4.1. a valid adequacy decision adopted by the Commissioner on the basis of Article 26 of the DP Law 2020;

2.4.2. the appropriate standard contractual clauses adopted by the Commissioner from time to time;

2.4.3. any other lawful data transfer mechanism, as laid down in DIFC Data Protection Laws.

2.5 **Standard Contractual Clauses**.

2.5.1. The DPA hereby incorporates by reference the DIFC SCCs. The Parties are deemed to have accepted, executed, and signed the DIFC SCCs where necessary in their entirety (including the appendices thereto).

2.5.2. The Parties agree that any references to clauses, appendices, and choices within this Section 2.5 (Standard Contractual Clauses) shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated DIFC SCCs as may be applicable from time to time pursuant to the DPA.

2.5.3. For the purposes of the DIFC SCCs and any substantially similar standard contractual clauses which may be adopted by the relevant authorities in the future:

(A) The DIFC SCCs shall be effective from the date of the DPA and shall remain in force in accordance with Section 5 (Termination and return or deletion) of the DPA.

(B) Clause 7: The Parties choose to include the optional docking clause;

(C) Clause 9: The Parties choose option 2, "General Written Authorization," and the time period, procedures for designation and notification of new Subprocessors are set forth in more detail in Exhibit B of the DPA;

(D) Clause 16: The Parties choose not to include the optional language for termination;

(E) Appendix 1: The content of Appendix 1 of the DIFC SCCs is set forth in Exhibit A of the DPA;

(F) Appendix 2: The content of Appendix 2 of the DIFC SCCs is as set forth in Section 2.2 of the DPA; and

(G) Appendix 3: The content of Appendix 3 of the DIFC SCCs is set out in Exhibit B of the DPA.

2.5.4. In cases where the DIFC SCCs apply and there is a conflict between the terms of the DPA and the terms of the DIFC SCCs, the terms of the DIFC SCCs shall prevail with regard to the Restricted Transfer in question.

3. **United Arab Emirates: Federal**.

3.1 **Definitions**.

3.1.1. "Data Office" means the UAE Data Office established by virtue of Decree-Law No. 44 of 2021.

3.1.2. "UAE Federal Data Protection Laws" includes the United Arab Emirates ("UAE") Personal Data Protection Law (Decree-Law No. 45 of 2021), Decree-Law No. 44 of 2021, and any corresponding decrees, regulations, or guidance.

3.2 **Personal Data Breach**. In addition to its obligations pursuant to Section 2.4 of the DPA, immediately upon providing notice of a Personal Data Breach, Collibra shall describe to Customer in as much detail as reasonably possible: (i) the form and causes of the Personal Data Breach, (ii) the potential and expected impact and consequences of such Personal Data Breach upon Customer and the affected Data Subjects, and (iii) the name and contact details of a contact point where more information can be obtained, which is: Data Protection Officer, email: privacy@collibra.com.

3.3 **Restricted Transfers**. With regard to any Restricted Transfer subject to UAE Federal Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

3.3.1. a valid adequacy decision adopted by the Data Office on the basis of Article 22 of Decree-Law No. 45 of 2021;

3.3.2. the appropriate standard contractual clauses adopted by the Data Office from time to time; or

3.3.3. any other lawful data transfer mechanism, as laid down in UAE Federal Data Protection Laws.

3.4 **General**. Collibra shall fully co-operate, on request, with the Data Office in the performance of its obligations under the UAE Federal Data Protection Laws.