DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is an integrant part of the contract for services ("**Agreement**") and it overrides any provision regarding processing of Personal Data included in any other contractual understanding of the parties.

A. PARTIES OF THE DPA

This DPA is concluded by and between

- The non-EXPLEO entity accepting the Data Processing Agreement, and which have entered into an agreement under which EXPLEO provides the Customer with a Service, as defined in the Agreement.
  (herein below the "**Data Controller**")

And

- The EXPLEO entity designated in the Agreement or Service agreement.
  (herein below the "**Data Processor**")

(Hereinafter jointly referred to as the "**Parties**")

B. PREAMBULE

The Parties recognise that for the data processing required to fulfil their own obligations and legitimate interests, the Parties are both qualified as separate Data Controllers, or the equivalent status by the applicable legislation. This data processing is related to the management of the business relationship, the pursue their respective legitimate interests and the compliance with their legal obligations (accounting, legal management, compliance due diligence, tax, declarations to authorities, etc). Each Data Controller guarantees the lawfulness and fairness of the processing carried out on its behalf and performs all necessary acts to this end in dealings with third parties, the supervisory authorities, and the other Party. For EXPLEO's data processing in such respect, the Data Controller confirms that it has acknowledged and presented to any required individual the Privacy Notice available at: https://expleo.com/global/en/privacy-notice/

For the provision of the services, the Parties seek to implement the requirements of legal framework in relation to any Applicable Data Protection Regulation as defined below.

1. DEFINITIONS AND INTERPRETATION

Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.1.1**.** ***"DPA"*** shall mean this Data Processing Agreement and all its schedules

1.1.2. ***"Agreement"*** shall mean the Contract concluded with the Processor for providing services.

1.1.3. "***Applicable Data Protection Regulations" or "Legislation"*** shall mean the relevant data protection and privacy laws or regulations ,including the General Data Protection Regulation – GDPR - or any other relevant regulation whether European or not, such as the Data Protection Act 2018 in United Kingdom, the Protection of Personal Information Act (POPIA) in South Africa, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, India's Personal Data Protection Bill, China's Personal Information Protection Law (PIPL), California Consumer Privacy Act (CPRA), Australia's Privacy Act 1988, and any other regulatory requirements to which the Controller is subject as well as any guidance and/or code of conduct issued or endorsed by the Data Protection Supervisory Authority.

1.1.4. "***Data Protection Supervisory Authority"*** shall mean the relevant supervisory authorities with responsibilities for data protection and/or privacy in all EXPLEO's jurisdiction in which the Services will be deployed.

1.1.5. "**EEA"** shall mean the European Economic Area

1.1.7. **"Services"** shall mean the services provided by the processor in relation to the processing of Personal Data as described in the Agreement;

1.1.8. “**Sub-processor”** shall mean any entity contracted by the Processor to which Personal Data, wholly or partially, are transfer for the purpose of providing services under the Agreement.

1.1.10 “**Standard Contractual Clauses”** shall mean the model contract clauses for international transfers issued on 4 June 2021 by the European Commission and where the UK GDPR applies, the EU SCCs as amended by the Annex on International Data Transfer to the European Commission's Standard Contractual Clauses, as published by the Kingdom's Information Commissioner's Office -UK (“CCT UK”) under S119A(1) of the UK Data Protection Act 2018, incorporated herein by reference.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly. The terms beginning with a capital letter in the Agreement will have the meaning assigned to them in this DPA and the Agreement. In case of contradiction or discrepancies, the definitions in the DPA shall prevail and replace any other definition included in the Agreement, in General Terms and Conditions or in any other contractual document.

2. PROCESSING OF PERSONAL DATA IN THE CONTEXT OF THE SERVICES

2.1 The Data Processor undertakes to process the Personal Data on behalf of the Data Controller in accordance with the Applicable Data Protection Regulation and for the purpose of providing the services provided for in the Contract. These services are fully described in the Agreement and in Appendix 1.

2.2 In compliance with Applicable Data Protection Regulation, the Processor reserves the right to process Customer’s data (whether it is Personal Data or not), in an aggregated and anonymised format, for its own legitimate interests.

2.3 The Data Processor undertakes to process the Personal Data in accordance with the documented instructions of the Data Controller, defined by the Data Processing Agreement. Except as described in Article 2.2, any changes to the Data Controller’s instructions shall be negotiated separately (taking into account the associated costs and the technical feasibility of such additional instructions).

2.4 The Data Processor undertakes to assist the Data Controller in fulfilling its legal obligations to the extent required by law and subject to reasonable fees for this assistance. The Data Processor shall provide such assistance if the Data Controller is unable to comply with its obligation by other means.

2.5 The Data Processor shall inform the Data Controller if, in its opinion, instructions provided under this Agreement are contrary to the Legislation.

2.6 If the data subjects, the competent authorities or any other third parties request information from the Data Processor concerning the Processing of the Data Controller’s Personal Data, the Data Processor shall forward this request to the Data Controller. The Data Processor may not and is not obliged in any way to act on behalf of or as a representative of the Data Controller and may not, in the absence of prior instructions or consent from the Data Controller, transfer or otherwise disclose the Personal Data or any other information relating to the processing of the Data Controller’s Personal Data to a third party. If the transfer or disclosure is required or authorised by law, no consent is required. If the Data Processor is required by the Applicable Data Protection Regulation to disclose Personal Data that it processes on behalf of the Data Controller, the Data Controller shall inform the Data Controller, within the limits provided by the Legislation.

2.7 The Processor shall have in place appropriate technical and organizational measures defined in Appendix 2, that the Data Controller has reviewed and confirm that it guarantees a level of security adapted to the risk related to the personal data processed. The Data Processor may modify the technical and organisational measures provided that the new technical and organisational measures are no less restrictive than the previous ones.

2.8 Upon becoming aware of it, the Data Processor shall promptly inform the Data Controller of any accidental or unauthorised access to the Personal Data processed on behalf of the Data Controller. That notification shall include all information that are mandatory under the Applicable Data Protection Regulation. The Data

Processor shall also provide reasonable assistance requested by the Data Controller to investigate the breach of security.

2.9 The Data Processor shall ensure that Personal Data processed on behalf of the Data Controller are only accessible by personnel who need such access to fulfil the Data Processor's obligations under this Agreement. The Data Processor shall ensure that such personnel are bound by an obligation of confidentiality.

2.10 If the California Consumer Privacy Act applies to this data processing, the Processor confirm that it performs the services for a purpose that meets the definition of "business purpose" in Section 1798.140(d)(5) of the California Consumer Privacy Act, as it may be modified, and do not subsequently sell any personal data.

3. SUBPROCESSORS AND TRANSFER OF PERSONAL DATA OUTSIDE EU

3.1. The Processor shall process Controller's Personal Data in the EEA, unless the contracting Expleo's entity is located outside of the EEA, or the Data Processor has received the consent of the Data Controller. If the Data Controller gives his consent to sub-processors located outside of EEA, the Data Processor shall ensure that these transfers are covered by the adequate measures, including Standard Contractual Clauses of the European Union (Module 3 – P2P).

3.2. If the contracting Expleo's entity is located outside of EEA, both Parties recognise the applicability of the Standard Contractual Clauses of the European Union, as incorporated in Appendix 3 (Module 2 – C2P). The Data Controller is the sole responsible of the obligation to perform a Transfer Impact Assessment and warrant that any authorized transfer is compliant with regulation.

3.3. The Data Controller authorizes the Processor to sub-process part of the data processing, to the sub-contractors defined in Appendix 1. The Data Processor may revoke, replace, or appoint other appropriate and reliable third-party data processors at its sole discretion, but will inform the Data Controller if a change is made to the list. If the Data Controller has legitimate reasons to refuse a new third-party data processor, it shall inform the Data Processor in writing within thirty days of receipt of the Data Processor's notification. The Processor shall enter into a written agreement with the Subcontractor that will contain terms and conditions at least as strict as those provided for in this DPA. The Sub-processor shall be under the obligation to implement equivalent security measures. The Data Processor shall remain liable to the Data Controller for the performance of the obligations of third-party data processors.

3.4. If the Controller is located in UK, the Parties recognize the applicability of the UK SCC Addendum, available in Appendix 4.

4. PERSONAL DATA BREACH

4.1. The Processor shall notify the Controller, as soon as possible, after it has become aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to Personal Data ("**Breach**").

4.2. The Processor shall immediately investigate the Breach and make its best efforts to prevent and to mitigate its effects. The Processor shall not release or publish any information, statement, communication or press release in relation to the Breach without Controller's written prior approval.

5. MEASURES FOLLOWING THE END OF THE PERSONAL DATA PROCESSING

5.1. Upon expiry of the Processing or Contract, the Data Processor undertakes, at the choice of the Data Controller as communicated to the Data Processor, to delete or return the Personal Data, including all copies. If no instruction is provided, the Data Processor will proceed to delete the data. The Data Controller accept that the return of all copies may be subject to reasonable fees.

5.2. At the request of the Data Controller, the Data Processor shall send a written confirmation regarding the measures taken concerning the above-mentioned data once the Processing has been completed. These provisions do not apply if the Data Processor is required to retain Personal Data by the Legislation or for documentation purposes. If it is technically impossible to delete or destroy Personal Data processed in electronic format, the Data Processor shall take reasonable measures to make such data inaccessible, non-recoverable and non-modifiable, any unjustified Processing being prohibited.

6. AUDIT RIGHTS

6.1. The Data Processor shall cooperate in a reasonable manner with the Data Controller and provide the available information in order to help the Data Controller better understand the security measures that the Data Processor has put in place. The Data Controller or any other auditor expressly appointed by the latter may carry out an on-site audit of the premises used to provide the services, provided that it does not disrupt the Data Processor's normal business and in accordance with the latter's security policies in order to reduce any risk for the Data Processor's other clients, and subject to reasonable fees.

6.2. Audits shall be carried out at the expense of the Data Controller and may be carried out once a year during the term of this Agreement, subject to the following provisions:

- (i) the audits do not include access to systems, data or information relating to the Data Processor's other clients;
- (ii) the audit shall be limited to information, documents and data relevant and related to the Processing of Personal Data by the Data Processor on behalf of the Data Controller pursuant to this Agreement; and
- (iii) audits shall not exceed two (2) working days, unless the Parties agree otherwise in writing and in advance or if special circumstances so require.

7. LIABILITY

7.1. The Data Controller guarantees the lawfulness and fairness of the Processing carried out on its behalf by the Data Processor and performs all necessary acts to this end in dealings with third parties, the supervisory authorities and the Data Processor. If changes in Applicable Data Protection Regulations result in additional costs to the Data Processor, the Data Processor may request compensation to recover these costs. Subject to technical feasibility, the right to negotiate compensation for costs as mentioned above will also apply if the Data Controller requests specific security measures. The Data Controller shall defend, indemnify and hold harmless the Data Processor and the Data Processor's officers, employees, successors and agents from and against claims, damages, liabilities, taxation, losses, costs, administrative fines and other expenses (including legal and judicial fees) resulting from any claim, allegation, demand, trial, action, order or other proceeding brought by a third party (including supervisory authorities) as a result of a breach of the Data Controller's duties pursuant to this Agreement and/or the Applicable Data Protection Regulation.

7.2. The Data Processor shall only be liable for direct damages caused to the Data Controller through its fault and to the persons whose Personal Data are processed as a result of a breach of the Applicable Data Protection Regulation or of the obligations provided for in the Agreement. In no event, the Data Processor shall have any liability arising out of indirect damages, such as loss of revenue, profit, or lost damages. In view of the purposes of the Processing and the categories of Personal Data processed by the Data Processor under the Agreement, the Data Processor's liability shall be limited to the fees perceived by the Supplier in the last 12 months or 50 000€, whichever is lower, in total for the Contract. This limitation precedes any other competing terms agreed between the Parties.

8. DURATION

8.1. This Agreement shall start on the date when the Agreement is signed and shall continue in full force and effect until the later of the termination or expiration of the Agreement; or the termination of the last of the Services or work packages to be performed pursuant to the Agreement.

8.2. The provisions of this DPA shall apply to any processing of Personal Data received prior to execution of the Agreement including during any transitional and/or migration phase.

9. FINAL CLAUSES

9.1. In case of contradiction or discrepancies, the rights and obligations laid down in this DPA will prevail and/or replace, depending on the situation any other contractual obligation included in the Agreement, in General Terms and Conditions or in any other contractual document signed between the Parties.

9.2. This DPA shall not under any circumstances assign, novate or otherwise transfer any of its rights or obligations without Controller prior express written consent.

9.3. The provisions of this DPA are severable. If any clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such clause or provision, and the rest of the DPA shall remain in full force and effect.

9.4. The provisions of this DPA shall be binding upon the parties and their respective successors and assignee.

9.5. This Agreement is governed by the laws of France. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Paris, unless otherwise specified in the Agreement.

APPENDIX 1 – DETAILS OF THE DATA PROCESSING

1. Categories of data subjects whose personal data is transferred

☒ Employees of Expleo ☒ Employees of the Third Party Other: None.

2. Categories of personal data transferred

☒ Business contact information Other: None.

3. 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.

Type of sensivite data: None. Safeguards: N.A.

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

☒ Continous ☐ One-off Other: N.A.

5. Nature and purpose of the processing

Description of the nature of data operations (ex. collection, use, erasure): Collection, use, erasure.

Description of the purpose of processig (ex.delivering the service as per the Agreement): Delivering the services described in the Agreement.

6. Purpose(s) of the data transfer and further processing

Reasons for the data transfer: None.

Description of any further data processing (ex. marketing operation): None.

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

Description of the timeline of the data processing (retention, erasure, rationale): Destruction at the end of the Agreement.

8. Agreed subprocessors

Name	Location	Nature of the service provided	Categories of personal data accessed	Confirmation that the sub-processor has signed a DPA and, if necessary, the SCC
None.				

<u>NOTE</u>: If the description of the data processing does not correspond to this Appendix, the Processor shall complete the form available at https://expleo.com/DP/DPA-Description-en and return it to dpo@expleogroup.com. The Parties agree that the new signed form will cancel and replace this Appendix.

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

As defined in Expleo Information Security Insurance Plan, as available at this url: https://expleo.com/DP/DPA-ISAP-en

APPENDIX 3 – STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

<u>SECTION II – OBLIGATIONS OF THE PARTIES</u>

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.

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[2] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(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.

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

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

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

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

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

Clause 9

Use of sub-processors

(a) SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 DAYS prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

(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.

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

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) 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.

(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[4];

(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

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

practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

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

15.1 Notification

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

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

Clause 18

(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 France.

(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): The Data Controller

Data importer(s): The Data Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Please refer to Appendix 1 – Details of the processing.

Categories of personal data transferred

Please refer to Appendix 1 – Details of the processing

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.

Please refer to Appendix 1 – Details of the processing

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

Please refer to the Agreement.

Nature of the processing

Please refer to Appendix 1 – Details of the processing

Purpose(s) of the data transfer and further processing

Please refer to Appendix 1 – Details of the processing

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

Please refer to Appendix 1 – Details of the processing

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

Please refer to Appendix 1 – Details of the processing

C. COMPETENT SUPERVISORY AUTHORITY

The Commission Nationale de L'informatiqe et des Libertés (FRANCE)

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

Please refer to Appendix 2.

ANNEX III – LIST OF SUB-PROCESSORS

Please refer to Appendix 1.

APPENDIX 4 – STANDARD CONTRACTUAL CLAUSES

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

ico.
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	Data of the signature	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As described in Appendix 1 of this DPA.	As described in Appendix 1 of this DPA.
Key Contact	As designated by the signature	As designated by the signature
Signature (if required for the purposes of Section 2)	Identical to the Agreement	Identical to the Agreement

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: Date of signature Reference (if any): The Agreement.

	Other identifier (if any): The Agreement. Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3	X	X	X	X	X	
4						

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: As described in Appendix 1 and 2.

Annex 1B: Description of Transfer: As described in Appendix 1.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Security Measure Addendum of the Framework Agreement.

Annex III: List of Sub processors (Modules 2 and 3 only): As described in Appendix 2.

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 **Error! Reference source not found.**: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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 **Error! Reference source not found.**.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section **Error! Reference source not found.** will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections **Error! Reference source not found.** to **Error! Reference source not found.** override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section **Error! Reference source not found.**, the provisions of Section **Error! Reference source not found.** will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section **Error! Reference source not found.** may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section **Error! Reference source not found.**) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

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

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section **Error! Reference source not found.**, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

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 **Error! Reference source not found.** of those Mandatory Clauses.