Partner Success. It's what we do.

Controller to Controller International Transfer Clauses

This Agreement is entered into by and between:

Westcon International Limited ("WINT"), a company registered in England and Wales (Company No. 04411310), with its registered office at Merchants House, Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire GL1 7YG,

and its subsidiaries listed below:

- **Westcon Group European Operations Limited** ("WGEO"), a company registered in England and Wales (Company No. 04411285), with its registered office at Merchants House, Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire GL1 7YG,
- **Westcon Group Middle East Holdings Limited** ("WGMH"), a company registered in England and Wales (Company No. 07319103), with its registered office at Merchants House, Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire GL1 7YG,
- **Westcon Group Africa Operations Limited** ("WGAF"), a company registered in England and Wales (Company No. 01264633), with its registered office at Merchants House, Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire GL1 7YG,
- **Westcon Group PTE Limited** (Singapore) ("WGPS"), a company registered in Singapore (Company No. 199903255M), with its registered office at 2 Shenton Way #18-01 SGX Centre, Singapore 068804,
- **Westcon Group Pty Limited** (Australia) ("WGPA"), a company registered in Australia (Company No. ABN 77 050 539 672), with its registered office at Unit 4, 39 Herbert Street St. Leonards, NSW 2065 Australia,
- **WG Services Inc** (USA) ("WGSI"), a company registered in Delaware, USA (Delaware File No. 6476691), with its address at 600 White Plains Road, 5th Floor, Tarrytown, NY 10591 United States,
- **Global Deployment Solutions LLC** (USA) ("GDS"), a company registered in Delaware, USA (Delaware File No. 6520991), with its address at 251 Little Falls Drive, Wilmington, New Castle, DE, 19808 United States.

(collectively the "**Group Affiliates**")

Vendor which shall be the legal name of a vendor of stock items as stated in the distribution contract between WINT or the Group Affiliates and the vendor in question.

Partner Success. It's what we do.

BACKGROUND:

A. **Westcon International Limited** ("WINT") and / or the Group Affiliates are engaged in business relationships with the vendors of stock items "**Vendors**" that involve the exchange and processing of personal data.

B. The Parties (including Vendors) are each Data Controllers as defined by the applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 ("GDPR").

C. In the course of the relationship, WINT and / or the Group Affiliates will need to export Personal Data from the European Economic Area, UK and / or Switzerland to the Vendor and / or its Affiliates in territories that are not considered "adequate" under the data protection laws of the EU, UK or Switzerland.

D. Accordingly, the parties need to enter into the cross-border clauses required by the EU, UK and Switzerland to ensure transfers to the non-adequate destinations is compliant with Applicable Privacy Law.

E. This Agreement incorporates the cross-border transfer clauses to ensure compliance with Applicable Privacy Law, including the GDPR.

Subsidiaries of WINT and their regions / territories:

WINT is the parent company of the Westcon Group, with the following subsidiaries responsible for processing personal data in the following regions/countries:

- **Europe:** Westcon Group European Operations Limited ("WGEO");
- **Middle East:** Westcon Group Middle East Holdings Limited ("WGMH");
- **Africa:** Westcon Group Africa Operations Limited ("WGAF");
- **Asia:** Westcon Group PTE Limited ("WGPS");
- **Australasia:** Westcon Group Pty Limited ("WGPA");
- **USA:** WG Services Inc ("WGSI"); and
- **Global Transactions:** Westcon GDS LLC ("WGDS").

AGREED TERMS:

1. Definitions

For the purpose of this Agreement, the following terms are defined as follows:

"Affiliates" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party. For the purposes of this definition, "control" means the direct or indirect ownership of more than fifty percent (50%) of the voting interests of

such entity or the power to direct the management and policies of such entity, whether through ownership, contract, or otherwise.

"Applicable Privacy Law" means all relevant data protection and privacy laws, regulations, and guidance, including GDPR.

"Effective Date" means 1st September 2025.

"European Economic Area" / "EEA" means the region consisting of the member states of the European Union together with Iceland, Liechtenstein, and Norway.

"Personal Data" means any information relating to an identified or identifiable natural person as defined by Applicable Privacy Law.

"Data Subject" means the individual to whom the Personal Data relates.

"Controller" means an entity that determines the purposes and means of the processing of Personal Data.

"Processor" means an entity that processes Personal Data on behalf of a Controller.

"Standard Clauses" refers to the EU Standard Contractual Clauses (Controller to Controller) as annexed at Annex 1.

2. Roles of the Parties

2.1 The Parties acknowledge that each is a Data Controller with respect to the Personal Data shared under this Agreement. Accordingly, each Party is responsible for its own compliance with applicable data protection laws in relation to the processing of Personal Data.

2.2 Each Party agrees to process Personal Data in compliance with Applicable Privacy Law, including but not limited to the GDPR.

2.3 The Parties agree to process Personal Data only for the purposes set out in this Agreement and as necessary to carry out their business operations.

3. Data Sharing and Processing

3.1 Each Party shall ensure that it has a lawful basis for processing in relation to Personal Data shared with the other Party.

3.2 The Parties agree to implement appropriate measures to safeguard the Personal Data during the exchange and processing.

4. Transfer of Personal Data

4.1 In the event that Personal Data is transferred from one Party to the other, or to a third country, the Parties will ensure that the transfer complies with Applicable Privacy Law.

4.2 Any export by WINT and / the Group Affiliates of Personal Data to the Vendor located in a destination not deemed "adequate" under the data protection laws of the territory the Personal Data was exported from:

4.2.1 from the European Economic Area (EEA) shall be subject to the Standard Clauses set out in Annex 1.

4.2.2 from the UK, shall be subject to the provisions of the UK Addendum to the Standard Clauses at Annex 2.

4.2.3 from Switzerland, shall be subject to the provisions of Annex 3.

5. Data Subject Rights

5.1 Each Party agrees to cooperate in responding to any data subject requests relating to Personal Data, including requests for access, rectification, erasure, and portability.

5.2 The Parties shall inform each other promptly if they receive any requests from data subjects regarding their Personal Data.

6. Data Security

6.1 Both Parties shall implement appropriate technical and organisational measures to ensure the security of Personal Data, including preventing unauthorized access, disclosure, or destruction of Personal Data.

6.2 Each Party shall immediately notify the other if there is a data breach involving Personal Data and cooperate fully to address and mitigate any potential harm.

7. Warranties

7.1 Each Party warrants that it:

7.1.1 comply with all applicable data protection laws and regulations in relation to the Personal Data; and

7.1.2 maintain appropriate security measures to protect the Personal Data.

8. Acceptance by Conduct

8.1 The Parties acknowledge and agree that, notwithstanding the absence of physical signatures, this Agreement and its Annexes shall be deemed accepted and binding upon the Parties by virtue of their ongoing business relationship, including but not limited to the exchange and processing of Personal Data in connection with the distribution of stock items.

8.2 The commencement or continuation of any business activities between WINT and/or the Group Affiliates and the Vendor, including the placing of orders, provision of quotes, or any other commercial engagement, shall constitute acceptance of the

terms of this Agreement, including the Standard Clauses set out in Annex 1, the UK Addendum in Annex 2, and the Swiss Addendum in Annex 3.

8.3 For the avoidance of doubt, such acceptance shall be treated as if the Agreement including any signature blocks in the annexures had been signed by the Parties on the Effective Date.

Partner Success. It's what we do.

ANNEX 1 - EU STANDARD CONTRACTUAL CLAUSES

The Parties agree to incorporate the following EU Standard Contractual Clauses as part of this Agreement for the transfer of Personal Data from the European Economic Area to outside of the EEA:

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Controller Established in a Third Country (Controller-to-Controller Transfers)

SECTION I

CLAUSE 1

Purpose and scope

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.

The Parties:

- 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 Exhibit I.A (hereinafter each 'data exporter'), and
- 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 Exhibit I.A (hereinafter each data importer)

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

These Clauses apply with respect to the transfer of personal data as specified in Exhibit I.B.

The Appendix to these Clauses containing the Exhibites 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.

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:

- Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- 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);
- Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
- Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
- Clause 13;
- Clause 15.1(c), (d) and (e);
- Clause 16(e);
- Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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.

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

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 Exhibit I.B.

[CLAUSE 7 – NOT USED]

Partner Success. It's what we do.

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.

8.1 Purpose limitation

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

- where it has obtained the data subject's prior consent;
- where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- where necessary in order to protect the vital interests of the data subject or of another natural person.

Transparency

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

- of its identity and contact details;
- of the categories of personal data processed;
- of the right to obtain a copy of these Clauses;

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

Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to

understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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

Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

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

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

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

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

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

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

8.6 Sensitive data

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

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these

Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

Documentation and compliance

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

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

CLAUSE 9

Use of sub-processors

N/A

Westcon Comstor

Partner Success. It's what we do.

CLAUSE 10

Data subject rights

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

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

- provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Exhibit I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
- rectify inaccurate or incomplete data concerning the data subject;
- erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

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

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

- inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
- implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

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

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

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

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.

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.

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:

- 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;
- refer the dispute to the competent courts within the meaning of Clause 18.

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.

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

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.

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

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.

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

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

CLAUSE 13

Supervision

(a) 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 Exhibit I.C, shall act as competent supervisory authority.

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.

Partner Success. It's what we do.

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.

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

- 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;
- 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;
- 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.

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.

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

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).

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:

- 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
- 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.

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.

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.).

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.

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).

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.

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.

Partner Success. It's what we do.

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.

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).

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

- 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;
- the data importer is in substantial or persistent breach of these Clauses; or
- 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.

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.

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.

Partner Success. It's what we do.

CLAUSE 17

Governing law

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

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.

The Parties agree that those shall be the courts of the Netherlands (specify Member State).

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.

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

Clause 19

Acceptance by Conduct

19.1 The Parties acknowledge and agree that, notwithstanding the absence of physical signatures, this Agreement and its Annexes shall be deemed accepted and binding upon the Parties by virtue of their ongoing business relationship, including but not limited to the exchange and processing of Personal Data in connection with the distribution of stock items.

19.2 The commencement or continuation of any business activities between WINT and/or the Group Affiliates and the Vendor, including the placing of orders, provision of quotes, or any other commercial engagement, shall constitute acceptance of the terms of this Agreement, including the Standard Clauses set out in Annex 1, the UK Addendum in Annex 2, and the Swiss Addendum in Annex 3.

Partner Success. It's what we do.

EXHIBIT I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Westcon International Limited and its subsidiaries

   Address: Merchants House, Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire, GL7 1YG

   Contact person's name, position and contact details: Sam Kershaw, Group Compliance Officer, complianceofficer@westcon.com

   Activities relevant to the data transferred under these Clauses: transfer of Personal Data for the purposes of carrying out business, including but not limited to placing orders, getting quotes and relaying information about customers and end users

   Signature and date: …

   Role (controller/processor): Controller

Data importer(s):

1. Name: Vendor

   Address: address set out in the distribution agreement with the Vendor

   Contact person's name, position and contact details: contact details advised by the Vendor from time to time

   Activities relevant to the data transferred under these Clauses: transfer of Personal Data for the purposes of carrying out business, including but not limited to placing orders, getting quotes and relaying information about customers and end users

   Signature and date: …

   Role (controller/processor): Controller

   2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Staff members of:
- Westcon
- End Users
- Westcon Customers

Categories of personal data transferred

- Identification data (name)
- Business contact details (phone number, email address, physical address)
- Employment details (e.g., job title,)
- System usage and access logs
- Any other personal data necessary for the performance of the contractual relationship

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.

- n/a

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

- Continuous

Nature of the processing

- For the performance of the distribution contract between the Parties

Purpose(s) of the data transfer and further processing

- Transfer of Personal Data for the purposes of carrying out business, including but not limited to placing orders, getting quotes and relaying information about customers and end users

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

- In accordance with the data retention policies of the Parties

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

- n/a

C. COMPETENT SUPERVISORY AUTHORITY

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

The supervisory authority of the Netherlands

Partner Success. It's what we do.

EXHIBIT II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Executive Summary

Westcon International, Ltd., together with its subsidiaries and affiliates (collectively, "Westcon-Comstor"), maintains an unwavering commitment to the highest standards of information security, in alignment with the ISO/IEC 27001:2022 framework. Recognizing the critical importance of protecting data across its supply chain in a dynamic regulatory environment, Westcon-Comstor has established a comprehensive Information Security Management System (ISMS) to govern its relationships with all vendors, ensuring consistent compliance, proactive risk management, and continuous enhancement of security controls.

As such, this policy describes the essential technical and organizational standards that Westcon-Comstor requires of its Vendors.

These measures are designed to maintain the confidentiality, integrity, and availability of data shared with, or accessed by, Vendors. Westcon-Comstor' s approach underscores its dedication to structured information protection, shared responsibility, and fostering a culture of security throughout its Vendor ecosystem.

Definitions—In the interest of clarity and to ensure alignment with ISO/IEC 27001:2022, the following definitions apply throughout this document:

- Vendor: Any third party, supplier, or service provider engaged by Westcon-Comstor to provide goods or services.
- Personal Data: Any information relating to an identified or identifiable natural person, as defined by applicable data protection laws.
- Personnel: Employees and authorized individual contractors of Westcon-Comstor' s Vendors.

1. Organization Information Security

Objective:

- Vendor must have an information security function that has been ratified and is supported by business leadership. Personnel are competent in information security.

Measures Include:

a) Vendor employs personnel with responsibility for information security.

b) Vendor has a comprehensive set of information security policies, approved by senior management and disseminated to all personnel.

c) Vendor security policies are reviewed at least annually and updated when needed.

d) Failure of personnel to follow information security policies is/can be treated as a disciplinary matter and lead to sanctions, including dismissal.

e) All Vendor personnel are given training in information security.

2. Information Security Management System

Objective:

- Vendor has an ISMS (Information Security Management System) in place to evaluate risks to the security of Personal Data, to manage the assessment and treatment of these risks, and to continually improve its information security.

Measures Include:

a) Vendor has deployed an ISMS to manage security professionally.

b) When risks are identified, the Vendor manages the implementation of appropriate security controls to treat and minimize the risks.

c) Establishing monitoring and performance measurements for continuous improvement

3. Physical Access

Objective:

- Physical access to Personal Data is protected.

Measures Include:

a) Any data centers are SOC 2 Type I and Type II compliant, and they comply with industry standards.

b) Facilities are controlled with various levels of defense including (but not limited to): alarms, CCTV, locked cages, biometric scanners, and guard stations that are manned 24/7. Only authorized representatives should have access to the premises.

c) Facilities and equipment are physically protected against natural disasters, malicious attacks and accidents.

d) Equipment or disk media containing Personal Data (including faulty or end of life disks) are not physically removed from the secure facilities unless securely erased prior to such removal or being transferred securely for destruction at a third-party site.

e) When Personal Data is copied electronically by Vendor outside secure facilities, appropriate physical security is maintained, and the data is strongly encrypted at all times.

4. System Access

Objective:

- Vendor data processing systems are used only by approved, authenticated users.

Measures Include:

a) Access to systems is granted only to Personnel and/or to permitted subcontractors (unless otherwise discussed and approved). Access is strictly limited as required for those persons to fulfil their function.

b) All users access systems with a unique identifier (user ID).

c) Vendor has established a password policy that prohibits the sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil defined minimum requirements and are stored in encrypted form. Each computer has a password-protected screensaver.

d) Vendor enforces 2-Factor Authentication (2FA) for all remote access.

e) Vendor has a thorough procedure to deactivate users and their access when a user leaves the company or a function.

f) An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is deployed to identify potential inappropriate access.

5. Data Access

Objective:

- Persons entitled to use data processing systems gain access only to the Personal Data that they are authorized to access.

Measures Include:

a) Vendor restricts Personnel access to files and programs on a "need-to-know" basis.

b) Personnel training covers access rights to and general guidelines on definition and use of Personal Data.

c) Where appropriate and practical, Vendor employs data minimization and pseudonymizing to reduce the likelihood of inappropriate access to Personal Data.

d) The production environment is separate from the development and testing environment

e) Vendor uses up-to-date anti-malware software on all appropriate computers and servers.

f) Vendor uses well-configured firewalls.

g) Vendor ensures that appropriate Personnel receive alerts and notifications from system software vendors and other sources of security advisories and installs system software patches regularly and efficiently.

6. Data Transmission

Objective:

- Prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during transfer.

Measures Include:

a) Connectivity to applications occurs over a secure TLS (HTTPS) connection.

b) Information is replicated real-time between production and primary data centers over an encrypted channel.

c) All replicated/backup data is stored in an encrypted format.

7. Confidentiality and Integrity

Objective:

- Personal Data remains confidential throughout processing and remains intact, complete and current during processing activities.

Measures Include:

a) Vendor has a formal background check procedure and carries out background checks on all new Personnel with access to Westcon-Comstor data.

b) Vendor has a formal product development security policy and uses a Secure Development Lifecycle (SDLC) that includes a wide range of security testing.

c) All changes to software are controlled and approved within a formal change control program that tracks, documents, tests, and approves change requests prior to implementation.

8. Availability

Objective:

- Data is protected from accidental destruction or loss, and there is timely access, restoration or availability to data in the event of an incident.

Measures Include:

a) Vendor uses a high level of redundancy so that an availability failure of a single system or component is unlikely to impact general availability.

b) Where necessary, multiple power supplies, generators on-site and with battery back-up to safeguard power availability.

c) Backups are encrypted and stored to an off-site location.

d) Vendor has a system in place to ensure that any failures of backup to operate correctly are flagged and dealt with.

e) Vendor performs restore tests from those backups at least annually.

f) Vendor has a business continuity plan in place which is regularly updated.

g) Vendor tests elements of its business continuity plan annually and learns from the results of such tests.

9. Incident Management

Objective:

- In the event of any security breach of data, the effect of the breach is minimized and the Westcon-Comstor is notified.

Measures Include:

a) Vendor maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified as incidents and response plans and procedures.

b) Vendor logs administrator and user activities to provide evidence in the event of an incident.

c) The clocks of all systems are synchronized to a single reference time source to aid investigation in the event of an incident.

d) Vendor regularly tests its incident response plan with "table-top" exercises and learns from tests and potential incidents to improve the plan.

e) In the event of a security breach, Vendor will notify Westcon-Comstor in accordance with applicable laws, after becoming aware of the security breach.

10. Artificial Intelligence

Objective:

- All Vendor-provided services and technologies that utilize Artificial Intelligence (AI) and Machine Learning (ML) adhere to standards for data privacy, security, and ethical use.

Measures Include:

a) Vendors must immediately disclose in writing any and all use of Artificial Intelligence and Machine Learning in relation to the provision of goods or services under this agreement, including any AI embedded within standard tooling. This includes AI used by the Vendor, its affiliates, or its subcontractors.

b) Vendors must limit Westcon-Comstor's data shared with AI systems to only what is absolutely necessary for the agreed-upon purpose. The Vendor must provide documentation on its data handling and minimization protocols upon request.

c) The Vendor is responsible for ensuring its use of AI complies with all applicable laws and regulations, including data privacy laws.

Partner Success. It's what we do.

ANNEX 2 - UK ADDENDUM TO STANDARD CONTRACTUAL CLAUSES

For Transfers of Personal Data from the European Economic Area (EEA) to the United Kingdom (UK)

1. **Standard Clauses:**
   The Parties shall ensure that all transfers of Personal Data from the EEA to the UK are made in accordance with the Standard Contractual Clauses, as supplemented by this Annex 2.
2. **Data Transfer:**
   In light of the UK's departure from the European Union, the Parties agree that the transfer of Personal Data from the EEA to the UK is subject to the UK's data protection regime, including the Data Protection Act 2018 and the UK GDPR, which mirrors the EU GDPR.
3. **Legal Basis for Transfer:**
   The legal basis for transferring Personal Data to the UK is the adequacy decision under Article 45 of the UK GDPR and the Standard Contractual Clauses as amended by this Addendum.

Part 1: Tables

Table 1: Parties

Start date	1st September 2025	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Westcon International Limited Trading name (if different): Westcon-Comstor Main address (if a company registered address): Merchants House Wilkinson Road, Love Lane Industrial Estate, Cirencester, Gloucestershire, GL7 1YG	Full legal name: Vendor Trading name (if different): trading name (if any) listed in the distribution contract with the Vendor Main address (if a company registered address): address listed in the distribution contract with the Vendor Official registration number (if any) (company number or similar identifier): Registration number

Partner Success. It's what we do.

	Official registration number (if any) (company number or similar identifier): 04411310	listed in the contract with the Vendor
Key Contact	Full Name (optional): Sam Kershaw Job Title: Group Compliance Officer Contact details including email: complianceofficer@westcon.com	Full Name (optional): Job Title: as advised by the Importer from time to time Contact details including email: as advised by the Importer from time to time
Signature (if required for the purposes of Section 2)		

Partner Success. It's what we do.

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: Effective Date Reference (if any): Other identifier (if any): 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						
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:
- Annex 1B: Description of Transfer:
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
- Annex III: List of Sub processors (Modules 2 and 3 only):

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 10 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 9 to 11 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 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) 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 18, 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:

Partner Success. It's what we do.

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.

Partner Success. It's what we do.

ANNEX 3 - SWITZERLAND ADDENDUM TO STANDARD CONTRACTUAL CLAUSES

For Transfers of Personal Data from the European Economic Area (EEA) to Switzerland

1. **Standard Clauses:**
   The Parties shall ensure that all transfers of Personal Data from the EEA to Switzerland are made in accordance with the Standard Contractual Clauses, as supplemented by this Annex 3.
2. **Data Transfer:**
   In accordance with the Swiss Federal Act on Data Protection (FADP) and the European Commission's adequacy decision on Switzerland, the Parties acknowledge that Switzerland ensures an adequate level of protection for Personal Data.
3. **Legal Basis for Transfer:**
   The legal basis for transferring Personal Data to Switzerland is the adequacy decision by the European Commission and the Standard Contractual Clauses as amended by this Addendum.

For the purposes of exports of personal data from Switzerland, in these standard contractual clauses:

1. The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c;
2. References to the GDPR are to be understood as references to the Swiss FADP; and
3. The standard contractual clauses also protect the data of legal entities until the entry into force of the revised FADP.
4. Exports of personal data from Switzerland shall be governed by and construed in accordance with the laws of Switzerland.