EU GDPR—2021 standard contractual clauses (SCCs) for the transfer of personal data to third countries—module two—controller to processor

STANDARD CONTRACTUAL CLAUSES (including UK Addendum)

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.

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

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

(b) Paragraph 3(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 Not used

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 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.

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The

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

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

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

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist 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.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

OR

(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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:** The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

OR

(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 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 ([5]);

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

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

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

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

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

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, and the data exporter agrees to notify , the data subject promptly (if necessary with the help of the data importer) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

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

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

(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.

Footnotes:

(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, 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 2021/915.

(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.

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

(4) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(5) 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.

If executed below by the data exporter or where not executed, where otherwise accepted by the data exporter, or by using the software, the parties agree to theses Standard Contractual Clauses, including the Annexes and, to the extent that the data exporter makes an international transfer of data to which UK Data Protection laws apply, the parties also agree that they are bound by the UK Addendum to the EU Commission Standard Contractual Clauses of even date.

Signed for and on behalf of: DATA EXPORTER

Print Name: ……

Position: …….

Signature: …….

Date: ……..

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s):

1.	Name: the contracting entity to PrinterLogic's licensing agreement. Address: as detailed on the licensing agreement/ order form or purchase order Contact person's name, position and contact details: as provided separately to PrinterLogic by the data exporter. Activities relevant to the data transferred under these Clauses: provision of software, software services and related support activities by PrinterLogic. Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1.	Name: PrinterLogic, Inc. (trading as Vasion) **"Vasion"** Address: 432 S. Tech Ridge Drive, St. George, UT 84770 Contact person's name, position and contact details: Martin Wright, General Counsel, martin.wright@vasion.com Activities relevant to the data transferred under these Clauses: provision of software, software services and related support activities by PrinterLogic. Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

The description of the transfer will differ depending on which application/product is being used, see below for further details.

PRINT DRIVER MANAGEMENT SOFTWARE AKA PRINTERLOGIC SAAS AND ON-PREMISE OFFERINGS ("PrinterLogic Software")

Categories of data subjects whose personal data is transferred

The personal data transferred concerns the following categories of data subjects: End users of the PrinterLogic application which may include employees and other personnel of the Data Exporter or of the customers of the Data Exporter, solely at the control and discretion of the Data Exporter or its end users.

Categories of personal data transferred

The personal data transferred may concern the following categories of data:

First name, last name, email address, title of print job, username and password.

The personal data transferred that may be transferred would not normally include any special categories of data, but data exporter is in control in this regard.

It should be noted that in Pull Printing mode the software will capture and store the title of a document which will be produced in print reports accessible to the licensor's IT personnel. The title of printed documents which may be reported (and stored) will be the title of the document as transmitted to the printer to be printed. This title may therefore contain special category data or personal data belonging to the data subject for which the data exporter may need to satisfy itself that it has obtained the express consent of the data subject to transfer in order to comply with its legal obligations under the General Data Protection Regulation 2016/679 (GDPR).

The controller is in control and may turn this function on or off as it sees fit.

If controller turns this function off, the Pull Printing mode within software will capture and temporarily store the title of a document which will be encrypted and not accessible to the licensor's IT personnel and will be temporarily stored until released by the transmitter of the document or for a period of time elected by the Controller until automatic expiry.

Data Exporter warrants to the Data Importer that where such consent must be obtained it has done so and that it has fully complied with its obligations in this regard.

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

The Data Exporter has contracted with the Data Importer for certain software services. In its use of the software services the Data Exporter will upload certain personal data into the software's database which may be stored at Controller's election either on servers (at the time of writing on Amazon Web Services AWS) outside of the EEA (which definition in the event that the United Kingdom leaves the European Union shall include servers in the United Kingdom), at the time of writing on Amazon Web Services (AWS) in the United States or within the EEA (which definition in the event that the United Kingdom leaves the European Union shall include servers in the United Kingdom). The data may be accessed, on the Data Exporter's request, by the Data Importer in order to provide technical support services. The personal data will be processed for the duration of the contract for software services and for a further period of thirty (30) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter.

Nature of the processing

The print management product does not typically actively use or access any data including personal data that data exporter uploads to its services and products, except where it is necessary to provide technical support to the Data Exporter at the Data Exporter's request.

Vasion's PrinterLogic Software (offered as a SaaS solution or an on-premise solution) performs two services that involve personal data.

1. Active Directory: A Vasion customer can establish an Active Directory within the PrinterLogic SaaS software that identifies authorized users for a specific printer along with what manner the authorized user may use the printer. (i.e. Printing in color or black only). The customer controls the information needed to run such authorizations (e.g. username, pin number, ID number, etc.)

2. Print Job Auditing and Reporting

   The software provides the customer with the following information via a print report.

   -Quantity of pages each department prints weekly, monthly or quarterly

   - Usage of any given printer to determine if a printer can be phased out

   -Actual cost of printing- itemized by department, location or printer

   -Identification of users who frequently initiate large print jobs

   -Notification of when a user prints a document labelled as "classified"

   -Overall printer usage data and printer consolidation guidance

   -Monitoring and reporting of all USB printing

Purpose(s) of the data transfer and further processing

For the on-premise solution, the PrinterLogic software is installed behind the customer's firewall and Vasion does not have access to the customer's network unless granted access during a product support request. For the SaaS solution, a client is installed locally that communicates with the PrinterLogic SaaS product hosted in Amazon Web Services which customers may elect to be stored on servers in the United States,or in the EEA (which in the event that the United Kingdom leaves the European Union shall exclude the United Kingdom). Although a customer may elect to store data on servers in the EEA, for purposes of software development and support, a limited number of PrinterLogic production engineers based in the United States may have access to data stored within servers in the EEA.

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

The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested

return of the data to the Data Exporter. Data stored within backup archives in AWS will be retained for 6 months after termination of services and permanently deleted thereafter.

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

At the time of writing the PrinterLogic SaaS solution is built and resides in Amazon Web Services (AWS). AWS is used to host the solution. Vasion does not utilize any other sub processors (or third-party providers) to access, process, or store customer data.

VASION BUSINESS PROCESS AUTOMATION PRODUCT (E-SIGNATURE, CAPTURE, WORKFLOW, and STORAGE) "Vasion Product"

Categories of data subjects whose personal data is transferred

The personal data transferred concerns the following categories of data subjects: End users of the Vasion product which may include employees and other personnel of the Data Exporter or of the customers of the Data Exporter, any other individual whose personal data is contained within the content uploaded to Vasion, always solely at the control and discretion of the Data Exporter or its end users.

Categories of personal data transferred

The personal data processed may concern the following categories of data: first name, last name, email address, title of printed document, username and password, IP addresses, email senders and recipients, and any other categories of personal data that maybe contained within the content uploaded to the Vasion product, solely at the discretion and control of the Data Exporter or its end users

Special categories of data

The personal data processed may contain the following special categories of data: any category of special data that may be contained within the content uploaded to the Vasion product, solely at the discretion and control of the Data Exporter or its end users.

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

The Data Exporter has contracted with the Data Importer for certain software services. In its use of the software services the Data Exporter will upload certain personal data into the software's database which will be stored on servers in the United States unless the Data Exporter is located in the United Kingdom or the EEA in which case the data will be stored on servers in the EEA. The data may be accessed, on the Data Exporter's request, by the Data Importer in order to provide technical support services. The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter.

Nature of the processing

The personal data processed will be subject to the following basic processing activities:

Use of the Vasion product does not typically require active use of or access to any data including personal data that Data Exporter or its end users upload to the product, except where it is necessary

for Vasion to provide technical support to the Data Exporter at the Data Exporter's request. Vasion merely offers technologies that its customers can use to store, retrieve, archive and share their data.

Data Exporter warrants to the Data importer that where consent must be obtained to process the personal data, it has obtained such consent and that it has fully complied with its obligations in this regard.

Purpose(s) of the data transfer and further processing

The Data Exporter and/ or its affiliate(s) have contracted with the Data Importer for a licence to use the Vasion product. In its use of the product the Data Exporter will upload content which may include personal data into the product which will be stored on servers according to where the Data Exporter is located. In accordance with the settings selected by the Data Exporter and its users, solely at their discretion, the Data Importer will permit the content including any personal data to be retrieved by the Data Exporter's users from (i) the product and (ii) via elected third party products and services. The Data Importer does not have access to the content, including any personal data, unless access is required for the provision of technical services and is authorised by the Data Exporter's IT representatives.

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

The personal data will be processed for the duration of the contract for products or services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter.

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

At the time of writing the Vasion solution is built and resides in Amazon Web Services (AWS). AWS is used to host the solution. PrinterLogic Software does not utilize any other sub processors (or third-party providers) to access, process, or store customer data.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

As determined by the parties.

ANNEX II

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

The technical and organisational measure will differ depending on which application/product is being used, see below for further details.

PRINT DRIVER MANAGEMENT SOFTWARE AKA PRINTERLOGIC SAAS AND ON-PREMISE OFFERINGS ("PrinterLogic Software")

PrinterLogic SaaS solution is built and resides in Amazon Web Services (AWS). Details of physical security implementation for AWS are found both at www.infrastructure.aws and https://aws.amazon.com/compliance/data-center/controls/

For the PrinterLogic Software, Vasion follows the ISO 27001 framework for governance and operations and further follows the OWASP SAMM framework for design, implementation and verification. Vasion anticipates obtaining ISO 27001 certification by Q3, 2022.

System Access Control:

Vasion prevents unauthorized access to data processing systems as follows;

- Supports role-based access control (RBAC) for system administrators. Multi-factor authentication is required to access the production environment containing customer data.
- Ensures that all computers accessing Customer data (this includes remote access) are password protected after boot sequences and have encrypted disks.
- Has dedicated user IDs for authentication against systems user management for every individual,
- Assigns individual user passwords for authentication,
- Ensures that the access control is supported by an authentication system,
- Only grants system access to Vasion's authorized personnel and/or to permitted employees of Vasion's subcontractors and strictly limits such persons' access to applications which process personal data as required for those persons to fulfil their function,
- Implements a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords,
- Ensures that passwords are always stored in encrypted form,
- Has a proper procedure to deactivate user accounts, when user leaves company or function, and
- Has a proper process to adjust administrator permissions when an administrator leaves company or function.

Processing of Personal Data:

Vasion protects Customer personal data it processes or stores in the PrinterLogic Software it provides to customers, as follows:

- Persons entitled to use data processing systems shall gain access only to the data to which they have a right of access, and personal data will not be copied, modified or removed without authorization in the course of processing. Including, without limitation, Vasion

  -Restricts access to files and programs based on a "need-to-know-basis",

  -Only grants access to Vasion personnel and assigns minimal permissions to access data as needed to fulfil their function.

- The responsibilities for the processing of personal data is clearly described (controller, processor, sub-processor, etc.)
- Vasion requires its employees and subcontractors (if applicable) to maintain confidentiality with respect to personal data and other confidential information of which they become aware in the course of providing services.
- Applicable Vasion employees receive appropriate privacy and data protection training to the extent that these matters are of importance to their work
- Personal data made available to Vasion in the course of its services is used solely for the agreed-upon purpose. Therefore, Vasion only processes personal data temporarily and for its intended purpose. At the end of the contract, after the completion of providing the agreed-upon services or upon the request of the customer, Vasion promptly returns or irretrievably deletes all customer data. In this regard, any supplemental agreements shall be taken into account.

Data Security and Preservation Controls:

Vasion takes the following measures to protect customer data.

- For encryption and protection of data during transmission and storage, all data is transported over https using TLS and at rest with AWS RDS database encryption using AES.
- Customer data is backed up daily/weekly. Daily backups are kept for seven days, weekly backups are kept for six months. Backup objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-3) or AWS KMS-managed keys (SSE-KMS)
- For data recovery and business resiliency, Vasion utilizes multiple availability zones within AWS. In the extreme event that all availability zones become unavailable, Vasion can utilize CloudFormation templates to rebuild infrastructure in a different region.
- Vasion separates customer data to prevent malicious or compromised users from affecting the service or data of another service.
- Vasion governs security to coordinate and direct its overall approach to the management of the service and information within industry standard security policies and security standards, defined responsibilities and risk based decision-making authority processes.

- Operational Security- Vasion has processes and procedures in place to ensure the operational security of the service provided including configuration and change management, security patch management, vulnerability management, protective monitoring, security incident management and secure decommissioning.
- Secure Development – Vasion ensures that all software it develops and provides as part of its service has been developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection.
- Vasion ensures that the methods used by administrators to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the service. Remote administration sessions must be encrypted, use at least two-factor for authentication, access to the systems administered must be restricted by IP addresses used by the Contractor by means of access control lists
- Vasion ensures to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. For the PrinterLogic SaaS solution, Vasion provides a Service Level Agreement identifying a minimum availability of 99.5% per month.

VASION BUSINESS PROCESS AUTOMATION PRODUCT (E-SIGNATURE, CAPTURE, WORKFLOW, and STORAGE) "Vasion Product"

Vasion Business Process Automation solution (including E-Signature, Capture, Workflow, and Storage) is built and resides in Amazon Web Services (AWS). Details of physical security implementation for AWS are found both at www.infrastructure.aws and https://aws.amazon.com/compliance/data-center/controls/

System Access Control:

Vasion prevents unauthorized access to data processing systems as follows;

- Supports role-based access control (RBAC) for system administrators. Multi-factor authentication is required to access the production environment containing customer data.
- Ensures that all computers accessing Customer data (this includes remote access) are password protected after boot sequences and have encrypted disks.
- Has dedicated user IDs for authentication against systems user management for every individual,
- Assigns individual user passwords for authentication,
- Ensures that the access control is supported by an authentication system,
- Only grants system access to Vasion's authorized personnel and/or to permitted employees of Vasion's subcontractors and strictly limits such persons' access to

applications which process personal data as required for those persons to fulfil their function,

- Implements a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords,
- Ensures that passwords are always stored in encrypted form,
- Has a proper procedure to deactivate user accounts, when user leaves company or function, and
- Has a proper process to adjust administrator permissions when an administrator leaves company or function.

Processing of Personal Data:

Vasion protects Customer personal data it processes or stores in the service it provides to customers, as follows:

- Persons entitled to use data processing systems shall gain access only to the data to which they have a right of access, and personal data will not be copied, modified or removed without authorization in the course of processing. Including, without limitation, Vasion

  -Restricts access to files and programs based on a "need-to-know-basis",

  -Only grants access to Vasion personnel and assigns minimal permissions to access data as needed to fulfil their function.
- The responsibilities for the processing of personal data is clearly described (controller, processor, sub-processor, etc.)
- Vasion requires its employees and subcontractors (if applicable) to maintain confidentiality with respect to personal data and other confidential information of which they become aware in the course of providing services.
- Applicable Vasion employees receive appropriate privacy and data protection training to the extent that these matters are of importance to their work
- Personal data made available to Vasion in the course of its services is used solely for the agreed-upon purpose. Therefore, Vasion only processes personal data temporarily and for its intended purpose. At the end of the contract, after the completion of providing the agreed-upon services or upon the request of the customer, Vasion promptly returns or irretrievably deletes all customer data. In this regard, any supplemental agreements shall be taken into account.

Data Security and Preservation Controls:

Vasion takes the following measures to protect customer data.

- For encryption and protection of data during transmission and storage, all data is transported over https using TLS and at rest with AWS RDS database encryption using AES.
- Customer data is backed up daily/weekly. Daily backups are kept for seven days, weekly backups are kept for six months. Backup objects are encrypted

using server-side encryption with either Amazon S3-managed keys (SSE-3) or AWS KMS-managed keys (SSE-KMS)

- For data recovery and business resiliency, Vasion utilizes multiple availability zones within AWS. In the extreme event that all availability zones become unavailable, Vasion can utilize CloudFormation templates to rebuild infrastructure in a different region.
- Vasion separates customer data to prevent malicious or compromised users from affecting the service or data of another service.
- Vasion governs security to coordinate and direct its overall approach to the management of the service and information within industry standard security policies and security standards, defined responsibilities and risk based decision-making authority processes.
- Operational Security- Vasion has processes and procedures in place to ensure the operational security of the service provided including configuration and change management, security patch management, vulnerability management, protective monitoring, security incident management and secure decommissioning.
- Secure Development – Vasion ensures that all software it develops and provides as part of its service has been developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection.
- Vasion ensures that the methods used by administrators to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the service. Remote administration sessions must be encrypted, use at least two-factor for authentication, access to the systems administered must be restricted by IP addresses used by the Contractor by means of access control lists
- Vasion ensures to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. Vasion provides a Service Level Agreement identifying a minimum availability of 99.5% per month.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1.	Name: Amazon Web Services Address: www.amazon.com Contact person's name, position and contact details: N/A Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud hosting.

ANNEX IV

Amendment to Standard Contractual Clauses

The parties hereby agree that the following amendments are made in accordance with Clause 2(a) of the Standard Contractual Clauses and shall apply as between the parties:

1. Documentation & Compliance (Clause 8.9)

Subclauses 8.9 (c), (d) and (e) are deleted in their entirety and replaced respectively with the following: :

" (c) The parties agree that the data importer shall in accordance with Article 28 of the GDPR and at the request of the data exporter once in any twelve month period submit its data-processing facilities for audit of the processing activities covered by these Standard Contractual Clauses which shall be carried out by a tier one auditing firm bound by a duty of confidentiality (which the data importer may require to be made directly with it).

(d) The parties agree that (i) where the data importer has achieved relevant certification it shall be permitted to substitute evidence of such certification in place of the requirement to submit to an audit under this clause and (ii) where the data importer has already undergone an audit within the previous three (3) year period then it shall be permitted to provide a copy of the resulting report to the data exporter as evidence of its compliance with the relevant data protection laws. The foregoing is subject to the provision that any resulting report shall be maintained as strictly confidential, an original copy is promptly provided to the importer by or on behalf of the exporter and all intellectual property rights in the report and its contents shall be deemed to be those of the importer.

(e) Any audit that is deemed necessary in accordance with this paragraph shall be subject to:

(i) the data exporter giving the data importer reasonable prior notice of such information request, audit and/or inspection and in any event not less than 10 working days;

(ii) the parties mutually agreeing upon the scope, timing and duration of the audit;

(iii) all parties ensuring that all information obtained or generated by the audit in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by applicable law);

(iv) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the data importers business, any sub-processors' business and the business of other customers of the data importer; and

(v) paying the data importer's reasonable charges for assisting with the provision of information and allowing for and contributing to inspections and audits."

2. Use of Subprocessors (Clause 9)

The following shall be inserted at the end of subclause 9(a):

"The parties agree that any changes, deletions or modifications made to the subprocessors may be notified to the data exporter via email unless the data importer has previously notified the data exporter in writing that it wishes to notify via publication on its website."

3. Liabilities (Clause 12)

3.1. A new subclause 12(h) is inserted as follows:

"Notwithstanding anything to the contrary in this Clause 12, if one party is held liable for a violation of the clauses committed by the other party or otherwise suffers any damage resulting from or connected to such violation, defaulting party shall be liable for direct damages, costs, charges, damages, expenses or losses the non-defaulting party has incurred provided that such liability shall be limited to direct damages only (excluding any indirect, exemplary, incidental, special or consequential damages) and shall be limited to a sum equal to the fees paid to Vasion by the Customer in the 12 months preceding the occurrence of the event triggering the damages."

3.2. A new subclause 12(i) is inserted as follows:

"Nothing in subclause 12(h) shall be construed so as to limit or restrict the rights of the data subject including the right to compensation to the extent that such restriction is not permitted by the GDPR or these Standard Contractual Clauses."

UK Addendum to the EU Commission Standard Contractual Clauses

This Addendum shall be applicable to all international 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 transfer.

Date of this Addendum:

1. The Clauses are dated on the date that they are executed or otherwise accepted by the data exporter.

This Addendum is effective from the same date as the Clauses.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex.

In addition, the following terms have the following meanings:

- This Addendum means this Addendum to the Clauses

- The Annex means the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021

- UK Data Protection Laws means 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 means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

- UK means the United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. 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

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a. for 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 transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 7 above, include (without limitation):

a. References to the "Clauses" means this Addendum as it incorporates the Clauses
b. 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."
c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
d. References to Regulation (EU) 2018/1725 are removed.
e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
h. Clause 18 is replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
i. The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

Executing this Addendum

12. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):

    a. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A: “By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:” and add the date (where all transfers are under the Addendum) “By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated” and add the date (where there are transfers both under the Clauses and under the Addendum) (or words to the same effect) and executing the Clauses; or

    b. By amending the Clauses in accordance with this Addendum, and executing those amended Clauses.