JOHNSON CONTROLS DATA PROCESSING ADDENDUM – JOHNSON CONTROLS AS PROCESSOR

This Data Processing Addendum, including its Schedules and Appendices, ("**DPA**") forms part of the Agreement or other written or electronic agreement between Johnson Controls (hereinafter referred to as "JCI") and Customer for the purchase by

Customer of services from JCI (identified as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.
All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, JCI may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW THIS DPA APPLIES

This DPA shall replace any conflicting terms relating to Processing of Personal Data contained in the Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"Canadian Privacy Laws" means the *Personal Information Protection and Electronic Documents Act* and the regulations thereto, and any applicable provincial legislation and regulations, including, where applicable, the *Personal Information Protection Act* (Alberta), the *Personal Information Protection Act* (B.C.), an *Act respecting the protection of personal information in the private sector* (Quebec) and an *Act to establish a legal framework for information technology* (Quebec), and any regulations to such statutes, each as amended from time-to-time.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that executed the Agreement.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, Canada, and the United States and its states, and the People's Republic of China, applicable to the Processing of Personal Data under the Agreement.
"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"UK GDPR: the GDPR, as amended and incorporated into the law of the United Kingdom ("UK") under the UK's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018.

"Personal Data" means any information relating to an identified or identifiable natural person where such information is information submitted by or for Customer to the Services.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"Security Practices Documentation" means the information available at this link: https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/johnson-controls-security-practices-rev-c.pdf

"JCI" means the JCI entity which is a party to the Agreement.

"JCI's Affiliates" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by, or is under common ownership or control with JCI. As used herein, "control" means the power to direct the management or affairs of an entity and "ownership" means the beneficial ownership of more than fifty percent (50%) of the voting equity securities or other equivalent voting interests of an entity.

"Standard Contractual Clauses" or "SCCs" means the agreement attached hereto as Schedule 3 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by JCI.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR,

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, JCI is the Processor and that JCI will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws and Regulations applicable to Customer, including any applicable requirement to provide notice to Data Subjects of the use of JCI as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including the obtaining of any consents required. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3 JCI's Processing of Personal Data. JCI shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) use of the Services and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. JCI shall not Process Personal Data on behalf of and in accordance with Customer's documented instructions where those instructions are in violation of applicable law

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by JCI is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS AND CO-OPERATION

Data Subject Request. JCI shall, on reasonable request from the Customer, and subject to any restrictions under applicable law, promptly notify Customer if JCI receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, JCI shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, JCI shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent JCI is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from JCI's provision of such assistance.

CO-OPERATION: Upon Customer's written request, JCI shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligations under Data Protection Laws and Regulations, and/or to assist in Customer's response to any enquiry, investigation or audit by any regulatory authority. To the extent legally permitted, Customer shall be responsible for any costs arising from JCI's provision of such co-operation and assistance.

4. JCI PERSONNEL

4.1 Confidentiality. JCI shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. JCI shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. JCI shall take commercially reasonable steps to ensure the reliability of any JCI personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. JCI shall ensure that JCI's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Data Protection Officer. Where obliged by law, JCI has appointed a data protection officer. The appointed person may be reached at privacy@jci.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) JCI's Affiliates may be retained as Sub-processors; and (b) JCI and JCI's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. JCI or a JCI Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. On written request from Customer, JCI shall make available to Customer the current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location. Addition of a new Sub-Processor will be notified by JCI to Customer by reasonable means, including email and other electronic means.

5.3Objection Right for New Sub-processors. If a new Sub-processor represents an unacceptable risk to the protection of the Personal Data, as determined by Customer acting reasonably, Customer may object to JCI's use of such new Sub-processor, by notifying JCI promptly in writing within ten (10) business days after notification of the new Sub-processor to Customer by JCI. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, JCI will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub- processor without unreasonably burdening Customer. If JCI is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by JCI without the use of the objected-to new Sub-processor by providing written notice to JCI.

5.4 Liability. JCI shall be liable for the acts and omissions of its Sub-processors to the same extent JCI would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 Controls for the Protection of Personal Data. JCI shall maintain appropriate technical, physical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Practices Documentation. JCI shall retain the right to update the Security Practices Documentation but not materially decrease overall measures.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

JCI maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, use of or access to Personal Data, transmitted, stored or otherwise Processed by JCI or its Sub-processors on behalf of Customer of which JCI becomes aware (a "**Personal Data Incident**"). JCI shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as JCI deems necessary and reasonable to remediate the cause of such a Personal Data Incident to the extent the remediation is within JCI's reasonable control. JCI will provide, without unreasonable delay, any information regarding the Personal Data Incident that is reasonably requested by the Customer, including all information required by Customer to comply with any reporting, recording and notification obligations applicable to Customer in connection with the Personal Data Incident, pursuant to Data Protection Laws and Regulations, as well as any information reasonably required by Customer to respond to any inquiries from relevant regulatory authorities and/or affected Data Subjects. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Data Subjects.

8. RETURN AND DELETION OF PERSONAL DATA

JCI shall return Personal Data (held in in any form, except electronic copies stored in the course of routine backup operations) to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the Agreement between Customer and JCI, provided that JCI's legal counsel may retain one archival copy for JCI's records. JCI shall not be required to delete Customer Personal Data to the extent JCI is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Data. Where JCI is required to retain Customer Personal Data as set forth in the preceding sentence, then JCI will notify Customer of such requirement, to the extent legally permitted.

9. LIMITATION OF LIABILITY

Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, JCI's and its Affiliates' total liability for all claims from Customer arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer, and, in particular, shall not be understood to apply individually and severally to Customer that is a contractual party to any such DPA.

Unless prohibited by law, to the extent that the Agreement does not include a "Limitation of Liability" section, IN NO EVENT SHALL JOHNSON CONTROLS AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS DPA, WHETHER ARISING OUT OF OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EXCEED THE TOTAL OF THE AMOUNTS PAID TO JCI PURSUANT TO THE AGREEMENT IN THE 12 MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 GDPR. JCI will Process Personal Data in accordance with the GDPR and UK GDPR requirements directly applicable to JCI's provision of its Services.

10.2 Data Protection Impact Assessment. Upon Customer's request, JCI shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR and, where applicable, the UK GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to JCI. JCI shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 10.2 of this DPA, to the extent required under the GDPR and UK GDPR.

10.3 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1, JCI makes available the transfer mechanism listed below which shall apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. The Standard Contractual Clauses set forth in Schedule 3 to this DPA

11. ADDITIONAL PROVISIONS WHEN CANADIAN PRIVACY LAWS APPLY

11.1 In situations where Canadian Privacy Laws apply, JCI will Process Personal Data in accordance with Canadian Privacy Laws.

11.2 Without limiting the generality of Section 2.2, in situations where Canadian Privacy Laws apply, regardless of whether Customer and/or the Data Subjects are located in Canada, Customer will provide any notices and obtain any consents required pursuant to Canadian Privacy Laws. In addition, where required, Customer will notify Data Subjects that their Personal Data may be transferred and stored outside of Canada and accessible to courts, law enforcement and national authorities in other countries, and Customer will obtain any consents required by Canadian Privacy Laws for JCI to transfer the Personal Data outside Canada and/or outside the Canadian province where the Customer and/or the Data Subjects are located.

11.3 Customer may contact JCI to request an audit of the procedures relevant to the protection of Personal Data, no more than once annually. Customer shall reimburse JCI for any time expended for any such audit at JCI's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and JCI shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by JCI. Customer shall promptly notify JCI with information regarding any non- compliance discovered during the course of an audit

12. Invalidity and Severability.

If any provision of these Terms is found by any court of administration body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect the other provisions of these Terms. Where permitted by applicable law, the Parties agree that in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the Parties would have agreed if they had taken the partial invalidity into consideration.

List of Schedules

Schedule 1: Transfer Mechanism for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

Schedule 4: UK Addendum to the Standard Contractual Clauses

SCHEDULE 1 - TRANSFER MECHANISM FOR EUROPEAN DATA TRANSFERS

1. ADDITIONAL TERMS FOR SCC SERVICES

1.1.Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Schedule 1 apply to Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed "data exporters".

1.2. Transfers subject to the UK GDPR: Where the transfer of Personal Data under this DPA is subject to the UK GDPR, Schedule 4 shall also apply.

1.3.Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to JCI for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement (b) use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. JCI shall not Process Personal Data on behalf of and in accordance with Customer's documented instructions where those instructions are in violation of applicable law.

1.4. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) JCI's Affiliates may be retained as Sub-processors; and (b) JCI and JCI's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. JCI shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA

1.5. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that JCI may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

1.6.Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by JCI to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by JCI beforehand; and, that such copies will be provided by JCI, in a manner to be determined in its discretion, only upon request by Customer.

1.7.Onwards transfers: Where Clause 8.8 of the Standard Contractual Clauses applies, the Customer understands and agrees that the appropriate "Module" is Module 3 (Transfer processor to processor) of the EU Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

1.8. Audits and Certifications. The parties agree that the audits described in Clauses 8.9(c)-(e) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Customer may contact JCI to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse JCI for any time expended for any such on-site audit at JCI's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and JCI shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by JCI. Customer shall promptly notify JCI with information regarding any non- compliance discovered during the course of an audit.

1.9. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by JCI to Customer only upon Customer's request.

1.10. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

SCHEDULE 2 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

JCI will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Customer in its use of the Services.

Duration of Processing

JCI will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Data subjects are determined and controlled by Customer through use of the Services, and may include various categories of Data Subjects as per the Services.

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion.

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

Module 2 - Controller to Processor

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [1] for the transfer of 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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional
Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

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

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 (10) business 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.([1]) 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([1]);

(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, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of 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 the Republic of Ireland.

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 the EU Member State in which the data exporter is established.

(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 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].*

[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]*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.*

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

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

Name: ____The data exporter is the legal entity identified as Customer herein.___ _

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

___*[please specify briefly your activities relevant to the transfer]*

Signature and date: _____

Role (controller):

2. …

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

Name: _ The data importer is the legal entity identified in the Agreement as providing Services to Customer._

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (processor):

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects are determined and controlled by the data exporter (the Customer) in its sole discretion, and may include various categories of Data Subjects as per the Services.

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

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.

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

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

The transfer may occur on a continuous or one-off basis depending on the Services performed by the data importer pursuant to the Agreement….

Nature of the processing

The data importer will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by the data exporter in its use of the Services.

Purpose(s) of the data transfer and further processing

The data importer will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by the data exporter in its use of the Services. …

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

The data importer will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

As outlined in clause 5.1 of the DPA, the data exporter agrees and acknowledges that the data importer may appoint JCI affiliates or other third-parties as Sub-processors in connection with the provision of the Services. The subject matter, nature and duration of the processing carried out by the Sub-processor will depend on the nature of the Services and such details will be notified to the data exporter in accordance with Clause 5.2 of the DPA….

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II

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

EXPLANATORY NOTE:

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data Processed by JCI as described at https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/johnson-controls-security-practices-rev-c.pdf or otherwise made reasonably available by data importer.

Examples of possible measures:

- *Measures of pseudonymisation and encryption of personal data*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and service*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*
- *Measures for user identification and authorisation*
- *Measures for the protection of data during transmission*
- *Measures for the protection of data during storage*
- *Measures for ensuring physical security of locations at which personal data are processed*
- *Measures for ensuring events logging*
- *Measures for ensuring system configuration, including default configuration*
- *Measures for internal IT and IT security governance and management*
- *Measures for certification/assurance of processes and products*
- *Measures for ensuring data minimisation*

- *Measures for ensuring data quality*
- *Measures for ensuring limited data retention*
- *Measures for ensuring accountability*
- *Measures for allowing data portability and ensuring erasure*

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

SCHEDULE 4– UK ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018
UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated [INSERT DATE.] This Addendum is effective from:

Choose one option and delete the other:

The same date as the EU Commission Standard Contractual Clauses, as set out in Schedule 3 to this DPA (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 Clauses those terms shall have the same meaning as in the AnnexClauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses as set out in Schedule 3 to this DPA.
The Clauses	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and as set out in Schedule 3 to this DPA.
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	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	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. In particular:

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.