Personal Data Processing Terms

These Personal Data Processing Terms ("Terms") are entered in between Johnson Controls, Inc.on behalf of itself and its Affiliates ("JCI") and [INSERT NAME OF PROCESSOR] ("Processor"), together ("Parties").

Preamble.

These Terms set forth confidentiality, security, and privacy requirements with respect to Personal Data Processed by Processor as part of the provision by Processor of the Services described in the Master Services Agreement ("MSA"). In the event of any conflict between the provisions of these Terms, its Annexes, and the provisions set forth in the MSA, the provisions that are more protective of Personal Data shall prevail.

1. **Definitions.** For the purposes of these Terms:

- "Affiliates" means all affiliated entities, including any parent, sister, daughter or subsidiary companies, of JCI or Processor. Any reference to Affiliates in these Terms shall also be deemed to include all Personnel of such Affiliates.
- "Annex" means the Annex to these Terms attached hereto and forming an integral part of these Terms.
- "Data Protection Rules" means the relevant national, federal, state and local laws and regulations that apply to the Processing of Personal Data, including but not limited to any applicable privacy and information security laws and regulations.
- "Data Subject" means an identified or identifiable natural person who can be identified directly or indirectly, including by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity. A legal person may qualify as Data Subject under the Data Protection Rules of specific jurisdictions, in which case such legal person shall also be considered a Data Subject for the purposes of these Terms.
- "Personal Data" means any information relating to a Data Subject.
- "Process", "Processing" or "Processed" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- "Personnel" means any employee, contractor, or agent.
- "Security Incident" means any: (i) transfer or disclosure to or access by third parties or Processing in breach of these Terms or the Data Protection Rules; (ii) loss of, or unauthorized access to or disclosure of, Personal Data resulting from breach of the safeguards described at Section 6 of these Terms or from a failure to establish such safeguards; (iii) or any event directly or indirectly affecting the confidentiality, integrity, or authenticity of Personal Data that is or was Processed by Processor on behalf of JCI or in connection with the Services.
- "Services" means the Services provided by Processor to JCI under the MSA.
- "Sub-Processor" means any data processor engaged by Processor or by any other Sub-Processor that Processes Personal Data on behalf of JCI. Any reference to a Sub-Processor in these Terms shall also be deemed to include all Personnel of the Sub-Processor.
- "Supervisory Authority" means a data protection authority or similar regulator as defined under Data Protection Rules.

2. JCI's Authority.

Processor shall only Process Personal Data for the business purpose of providing the Services and all such Processing shall be strictly in compliance with the requirements set out in these Terms and in compliance with JCI's instructions as issued from time to time.

3. Processor Obligations.

Processor shall, and Processor shall ensure that its Personnel, Affiliates and Sub-Processors shall, Process all Personal Data fairly and lawfully, respect the privacy of Data Subjects and comply with all Data Protection Rules. Processor shall also ensure that its Personnel, Affiliates and Sub-Processors shall have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Processor shall not (i) obtain any rights to any Personal Data by virtue of providing the Services, (ii) transfer or disclose any Personal Data (in part or in whole) to any third party, except as stipulated in these Terms, or (iii) Process or use any Personal Data for its own purposes or benefit. Processor shall notify JCI of any change in operations or legislation which is likely to have an adverse effect on its ability to comply with these Terms.

4. International Transfers.

4.1. General. All transfers of Personal Data shall be in compliance with the Data Protection Rules applying to JCI or the JCI Affiliate which exports the Personal Data. Onward transfers of Personal Data by Processor shall be made in strict compliance with such Data Protection Rules. Processor shall provide to JCI at least ninety (90) days of advance written notice prior to transferring Personal Data outside the country where the relevant Data Subjects reside.

4.2. Transfers from EEA Countries. All transfers of Personal Data from the European Economic Area or Switzerland, hereinafter referred to collectively as the "EEA", to countries outside the EEA must be in strict compliance with the Data Protection Rules applying to the JCI Affiliate located in the EEA which exports the Personal Data. For this purpose, Processor and/or its Affiliates shall enter into the European Commission approved Standard Clauses for the transfer of personal data to processors located outside the EEA ("Model Contract") with JCI as needed to satisfy cross-border transfer obligations under applicable Data Protection Rules. The Model Contract shall be annexed to these Terms. A Model Contract may not be necessary in case the Personal Data is transferred to a country that has been identified by the European Commission as providing adequate protection to Personal Data or to a Processor and/or its Affiliates offering protection to Personal Data under applicable Binding Corporate Rules. If the Personal Data is transferred to the United States, and Processor has self certified to the EU-US and/or Swiss-US Privacy Shield Framework (as applicable), the Model Contract may not be necessary and the following will apply: Processor represents and warrants that it has self-certified to the EU-US and/or Swiss-US Privacy Shield Framework (as applicable) and will maintain such certification continually for the duration of these Terms, including any extensions or option periods, and that it will adhere to the U.S. Department of Commerce Privacy Shield Principles in performance of these Terms. If the EU-US or Swiss-US Privacy Shield Framework is ruled invalid by a competent court or institution, Processor and/or its Affiliates shall immediately enter into the Model Contract with JCI.

4.3. Onward Transfers. Onwards transfers of Personal Data by Processor shall be made in strict compliance with Data Protection Rules and – if applicable - the annexed Model Contract or the EU-US or Swiss-US Privacy Shield Framework.

5. Third Parties and Sub-Processors.

Processor may subcontract work that relates to Personal Data under these Terms only in accordance with JCI's instructions. Processor represents that it shall provide a list of all relevant Sub-Processors (i) prior to starting Processing, (ii) at a later date when Processor uses a new Sub-Processor, and (iii) at any time upon JCI's request. This list should also include all geographic

locations where Processing may take place. JCI may object to the use of a new Sub-Processor in writing if the new Sub-Processor represents an unacceptable risk to the protection of the Personal Data as determined by JCI.

All Sub-Processors must comply with applicable Data Protection Rules and must be bound by an agreement that is substantially similar to these Terms, including but not limited to substantially the same provisions on international transfers, confidentiality and information security, cooperation and enquiries, Security Incidents and breach notification, and inspection and audit rights. JCI shall be granted the same rights granted in these Terms vis-à-vis the Sub-Processor. The Sub-Processing agreement shall be provided to JCI promptly upon request. Processor shall remain liable for all acts or omissions of Sub-Processors with respect to the Personal Data.

6. Confidentiality and Information Security.

Processor shall keep Personal Data strictly confidential and represents that it has implemented adequate physical, technical and organizational measures, which are reasonable based upon the sensitivity of the Personal Data and/or necessary to secure the Personal Data and to prevent unauthorized access, disclosure, alteration or loss of the same in light of the relevant risks presented by the Processing. In particular, such measures shall include, but shall not be limited to:

- Preventing access by unauthorized persons to Processing facilities and systems, where Personal Data is Processed or used (physical access control).
- Preventing unauthorized use of Processing systems (admission control).
- Ensuring that those persons authorized to use a Processing system are only able to access Personal Data within the scope of their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization during Processing or use and after recording (virtual access control).
- Ensuring that, during electronic transfer, transportation or when being saved to data carriers, Personal Data cannot be read, copied, modified or deleted without authorization, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control).
- Ensuring that it is possible to check and ascertain whether and by whom Personal Data has been accessed, modified or deleted from Processing systems (input control), and ensuring that such access, modification and deletion of Personal Data is, in fact, monitored for any unusual or suspicious activities.
- Ensuring that Personal Data Processed under these Terms can only be Processed in accordance with the instructions issued by JCI (assignment control).
- Ensuring that Personal Data is protected against accidental malfunctions or loss (availability control).
- Ensuring that Personal Data collected for different purposes can be Processed separately (separation control).
- Maintaining a process for regularly testing, assessing and evaluating the effectiveness of physical, technical and organizational measures to ensure the security of the Processing.
- Ensuring that Processor has developed and implemented appropriate privacy and data protection policies and procedures, and that all Personnel who are involved in Processing the Personal Data have been appropriately trained to Process the Personal Data in accordance with such policies and procedures as well as in accordance with these Terms and applicable Data Protection Rules.
- Ensuring that disposal of Personal Data is accordance with Section 10 of these Terms is implemented in a secure manner.

At the request of JCI, Processor shall provide the former with a comprehensive and up-to-date confidentiality and information security concept relating to the Processing of Personal Data under these Terms. In the event that JCI requires Processor to amend any confidentiality and information security measures, Processor shall cooperate with JCI to implement such measures as soon as practicable.

Processor shall ensure that its Personnel, Affiliates' Personnel and Sub-Processors' Personnel are subject to legally binding confidentiality and information security obligations that meet or exceed the requirements set forth in these Terms and that survive the termination of their employment.

7. Cooperation and Enquiries.

The Parties shall co-operate with each other to promptly and effectively handle enquiries, complaints, audits or claims from any court, governmental official, Supervisory Authority, third parties or individuals (including but not limited to the Data Subjects). Processor shall inform JCI of any such enquiry, complaint or claim within 24 hours of Processor's receipt of such enquiry, complaint or claim, unless prohibited under national law. Processor shall – specifically in such cases – provide all information that is necessary for JCI to fulfill its obligations under the applicable Data Protection Rules and these Terms, including the completion of privacy impact assessments and including making available all information necessary to demonstrate compliance by Processor with its obligations under these Terms. The Parties shall cooperate to respond appropriately to the exercise of any rights of any Data Subjects, in a timely manner, including with respect to objection to Processing, access, rectification, erasure, restriction, blocking, withdrawing consent, automated decision-making, profiling and portability of Personal Data. If a Data Subject seeks to object to the Processing of, or seeks to access, rectify, erase, restrict or block Personal Data pertaining to him or her, or exercise any rights regarding automated decision-making, withdrawal of consent, profiling or portability, Processor shall co-operate with JCI to take the actions required under the Data Protection Rules in accordance with JCI's instructions.

8. Security Incidents and Breach Notification

Processor shall inform JCI as soon as possible and in any event within 24 hours of discovering a Security Incident or a potential Security Incident, including a Security Incident concerning business contact information. The information should provide the details of the Security Incident, including (i) information on the Data Subjects affected, including categories and numbers of Data Subjects affected, and jurisdiction(s) where Data Subjects are located; (ii) a description of the nature of Security Incident, including the day on which or time period during which the Security Incident occurred and the cause of the Security Incident if known; (iii) a description of the Personal Data that was compromised or potentially compromised; (iv) the identity and contact details of a contact person who can answer questions on behalf of the Processor; (v) the likely consequences of the Security Incident, including an assessment of the risk of harm to Data Subjects; and (vi) a description of the steps taken to reduce the risk of harm to the Data Subjects, as well as the steps intended to be taken and/or recommended by the Processor to minimize possible harm. Processor shall provide all additional information reasonably requested or required by JCI in connection with the Security Incident. Processor shall fully cooperate with JCI in connection with the investigation, containment and remediation of the Security Incident.

In addition, Processor will inform JCI within 24 hours if (i) Processor or its Personnel, Affiliates or Sub-Processors infringe Data Protection Rules or obligations under these Terms, (ii) significant failures occur during the Processing, or (iii) there is reasonable suspicion of the occurrence of an event as defined under (i) and (ii) of this paragraph. In consultation with JCI, Processor must take appropriate measures to secure Personal Data and limit any possible detrimental effect on Data Subjects.

The Parties are aware that Data Protection Rules may impose a duty to inform the Supervisory Authority or affected Data Subjects in the event of a Security Incident. Processor shall assist JCI in providing notice to the Supervisory Authority and affected Data Subjects and meeting any other requirements that may apply to JCI or any of its Affiliates pursuant to applicable Data Protection Rules. Processor shall notify JCI of any Security Incident prior to notifying any Supervisory Authority or Data Subject of the Security Incident, and the form and content of such notification(s) shall be subject to JCI's approval (subject to any mandatory form or content requirements under applicable Data Protection Rules), unless Processor cannot provide such advance notification to JCI and also comply with its legal obligations under applicable Data Protection Rules.

9. Inspection & Audit Rights.

Upon prior written notice, JCI may inspect Processor's operating facilities or conduct an audit to ascertain compliance with these Terms. This right includes, but is not limited to, the verification of whether Processor has implemented appropriate physical, technical and organizational controls and procedures to protect the confidentiality, integrity and security of the Personal Data. The inspection may be carried out by JCI, or an independent third party, or by means of a self-assessment process approved by JCI. Processor shall fully cooperate with any such audit and investigation procedures initiated by JCI.

10. Retention, Return and Deletion of Personal Data:

These Terms shall remain in force until the latest of: (i) the date the Services provided under the MSA are completed, (ii) all Personal Data has been returned to JCI and/or irrevocably deleted/destroyed, (iii) the expiration or termination of the MSA, or (iv) the expiration of any confidentiality obligations.

The Processor shall not retain Personal Data (or any documents or records containing Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of the MSA.

Upon expiration of the purposes for Processing the Personal Data, termination of these Terms, or at any time at the request of JCI, Processor, at the discretion of JCI, shall return to JCI or irrevocably destroy and delete all Personal Data and other materials containing Personal Data, including existing copies of the Personal Data, subject to Processing, unless otherwise required by applicable law. Additionally, all Personal Data should be irretrievably expunged from any computer, server, media or storage device, word processor or similar device in which it was stored or Processed by Processor or by its Sub-Processors. Processor shall certify that this has been done upon JCI's request. Processor shall warrant that it, its Personnel, Affiliates and any Sub-Processors shall continue to be bound by their obligations of confidentiality after termination of the MSA or these Terms.

11. Indemnity.

In the event of non-compliance with any of the provisions of these Terms on the part of Processor or its Personnel, Affiliates or Sub-Processors, Processor shall defend, indemnify, and hold harmless JCI, its Affiliates and its directors, officers and Personnel from and against any third party claims, actions, applications, demands, complaints, damages, or liabilities (including reasonable legal fees and disbursements) arising from such non-compliance.

12. Governing Law.

These Terms are governed by the law of the country that governs the MSA and the Parties submit to the jurisdiction of the courts referred to in the MSA without regard to provisions related to conflicts of law.

13. Variation of the Terms.

These Terms may only be modified by a written amendment signed by each of the Parties.

14. 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.

IN WITNESS WHEREOF, the Parties have executed these Terms as of the last dated signature below.

Executed by	Executed by
Johnson Controls, Inc.	[INSERT NAME OF PROCESSOR]
Authorized Signature:	Authorized Signature:
_____	_____
Name/Title: _____	Name/Title: _____
Date: _____	Date: _____

ANNEX – Model Contract for Transfers from EEA Countries

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: The **Johnson Controls affiliates** established in the European Economic Area ("EEA") as referenced in the Only Schedule attached hereto and legally represented by Power of Attorney set forth in the Intra-Group Agreement dated 1st July 2017, by Johnson Controls Inc. with
Address: 5757 North Green Bay Avenue, Milwaukee, Wisconsin 53209, USA

(the data **exporter**)

And

Name of the data importing organisation: .....
Address: .....
Tel.:.....; fax:.....; e-mail:.....

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
The EEA-based affiliates of Johnson Controls., a global diversified company in the fire & security, building and automotive industries.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
……
……

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
……
……

Categories of data
The personal data transferred concern the following categories of data (please specify):
……
……

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
……
……

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
……
……

DATA EXPORTER
Name:……
Authorised Signature ……

DATA IMPORTER
Name:……
Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

……
……
……
……

DATA EXPORTER
Name:……
Authorised Signature ……

DATA IMPORTER
Name:……
Authorised Signature ……

ONLY SCHEDULE – DATA EXPORTER ENTITIES

The Johnson Controls affiliates referenced in this Only Schedule are party to these Standard Contractual Clauses as data exporter. This Only Schedule reflects the EEA based Johnson Controls affiliates that are party to the Intra-Group Agreement dated 1st July 2017 and which are referenced in Schedule 1 to that agreement and which is available at www.johnsoncontrols.com/IGA. Processor understands that additional Johnson Controls affiliates (not identified at the time of the execution of these Standard Contractual Clauses) may from time to time become party to the aforementioned Intra-Group Agreement. Parties agree that such additional Johnson Controls affiliates will, through their accession to the aforementioned Intra-Group Agreement become party to these Standard Contractual Clauses for the transfer of personal data to Processor and Processor agrees to process and protect personal data it imports from such data exporters under these Standard Contractual Clauses.