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 Schedules, 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.
- "Controller" means a natural or legal person that determines the purposes and means of Processing of Personal Data.
- "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, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, sale, sharing or otherwise making available, alignment or combination, blocking, erasure or destruction.
- "Processor" means a natural or legal person that processes Personal Data on behalf of a controller including as applicable any "service provider" as that term is defined in relevant Data Protection Rules.
- "Personnel" means any employee, contractor, or agent.
- "Schedule 1" and "Schedule 2" mean the Schedules to these Terms attached hereto and forming an integral part of these Terms.
- "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. Processor hereby grants to JCI the right to take reasonable and appropriate steps in addition to those specified in these Terms as necessary to (i) ensure that Processor, its Personnel, Affiliates, Sub-Processors, contractors, and/or third parties Process all Personal Data strictly in compliance with the requirements set out in these Terms, JCI's instructions, and the Data Protection Rules; and (ii) stop and remediate any unauthorized Processing of Personal Data by Processor, its Personnel, Affiliates, Sub-Processors, contractors, and/or third parties, in each case as determined by JCI in its reasonable discretion.

3. Processor Obligations.

Processor shall, and Processor shall ensure that its Personnel, Affiliates and Sub-Processors shall Process all Personal Data fairly, lawfully, and exclusively for the purpose of providing the Services and 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 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.

4.2. Transfers from EEA Countries and the UK. All transfers of Personal Data from: i) the European Economic Area or Switzerland, hereinafter referred to collectively as the "EEA"; or ii) from the United Kingdom ("UK"), to countries outside the EEA or UK must be in strict compliance with the Data Protection Rules applying to the JCI Affiliate located in the EEA or UK which exports the Personal Data. For this purpose, Processor and/or its Affiliates shall enter into the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 ("Model Contract") with JCI as needed to satisfy cross-border transfer obligations under applicable Data Protection Rules. In circumstances where the JCI affiliate is a controller and Processor is a processor with respect to Personal Data, Module Two of the Model Contract (for controller to processor transfers) shall apply, the terms of which are hereby incorporated by reference and subject to the terms of Schedule 1. In circumstances where the JCI affiliate has entered into a contract with a JCI customer and is processing Personal Data as a processor on behalf of said customer, Module Three of the Model Contract (for processor to processor transfers) shall apply to any transfers of Personal Data between the JCI affiliate and Processor, the terms of which are hereby incorporated by reference and subject to the terms of Schedule 1. The Annexes to the Model Contract shall be annexed to these Terms as Schedule 1. Where Personal Data is subject to the Data Protection Rules of the UK, Processor and/or its affiliates shall, in addition to the Model Contract, enter into the 'UK Addendum to the EU Commission Standard Contractual Clauses' ("UK Addendum"). The UK Addendum shall be annexed to these Terms as Schedule 2. 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 or the UK Government 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. .

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 at Schedule 1 . Where onwards transfers are subject to the Model Contract incorporated by reference in accordance with Section 4.2 of these Terms, the Processor shall ensure that the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Three for processor to processor transfers) are incorporated into the contract with the Sub-Processor before the onwards transfer takes place.

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 limitations on Processing, compliance with Data Protection Rules, international transfers, confidentiality and information security, cooperation and enquiries, Security Incidents and breach notification, inspection and audit rights, and rights granted to JCI to (i) take reasonable and appropriate steps required, in JCI's reasonable discretion, to ensure compliance with these Terms, JCI's instructions, and the Data Protection Rules and (ii) stop and remediate unauthorized Processing of Personal Data. 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.

Processor must put in place adequate processes and procedures to receive and process Data Subject requests related to the exercise of any rights of any Data Subjects provided by the Data Protection Rules, including with respect to objection to Processing, access, rectification/correction, erasure/deletion, restriction/limitation, blocking, withdrawing consent, opting-in or opting-out of the sale or sharing, automated decision-making, profiling and portability of Personal Data. Processor shall notify JCI promptly upon receipt of a Data Subject request to exercise any rights such rights. If a Data Subject seeks to exercise such rights, Processor shall co-operate with JCI to take all actions JCI determines are 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. 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; (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: _____

SCHEDULE 1 – Model Contract for Transfers from EEA Countries

1. Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Two for controller to processor transfers)

1.1. In relation to Personal Data transferred subject to Module Two of the Model Contract in accordance with Section 4.2 of these Terms:

(a) the optional clause 7 is excluded;

(b) for clause 9(a), option 2 (general written authorisation) is selected and the specified time period is thirty (30) days;

(c) the optional language at clause 11(a) (redress) is excluded**;**

(d) for clause 17, the first option is used and the law of Belgium is selected; and

(e) for clause 18(b), the courts of Belgium are selected.

2. Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Three for processor to processor transfers)

2.1. In relation to Personal Data transferred subject to Module Three of the Model Contract in accordance with Section 4.2 of these Terms:

(a) the optional clause 7 is excluded;

(b) for clause 9(a), option 2 (general written authorisation) is selected and the specified time period is thirty (30) days;

(c) the optional language at clause 11(a) (redress) is excluded;

(d) for clause 17, the first option is used and the law of Belgium is selected; and

(e) for clause 18(b), the courts of Belgium are selected.

ANNEXES TO THE MODEL CONTRACT

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 **Johnson Controls affiliates** established in the European Economic Area ("EEA") as referenced in Appendix A 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]

_____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses:

___ The EEA-based affiliates of Johnson Controls., a global diversified company in the fire & security, building and technology industries.

_____

Signature and date: _____

Role (controller/processor):

2. …

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

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): 2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

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.

...

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

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

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

...

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

...

C. COMPETENT SUPERVISORY AUTHORITY

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

...

APPENDIX A – DATA EXPORTER ENTITIES

The Johnson Controls affiliates referenced in this Appendix A are party to the Model Contract as data exporter. This Appendix A 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 the Model Contract) 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 the Model Contract for the transfer of personal data to Processor and Processor agrees to process and protect personal data it imports from such data exporters under the Model Contract.

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.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[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 services

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 2 – UK Addendum to the Model Contract

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0)

This Addendum (herein referred to as the "IDTA") has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

Table 1: Parties	
Start date	The start date is the same as the start date of the Standard Contractual Clauses in Schedule 1.
Parties' details	The parties' details are the same as specified in Schedule 1.
Key contact	The key contacts are the same as specified in Schedule 1.
Signature	The parties' signatures to the Standard Contractual Clauses in Schedule 1 are also deemed execution of this IDTA.
Table 2: Selected SCCs, Modules and Selected Clauses	
The Addendum EU SCCs are the Standard Contractual Clauses as specified in Schedule 1, including the Appendix Information.	
Table 3: Appendix Information	
The information provided as Appendix Information to the Standard Contractual Clauses as detailed in Schedule 1.	
Table 4: Ending this IDTA when the Approved Addendum changes	
The exporter may end this IDTA when the Approved Addendum changes.	

PART 2: MANDATORY CLAUSES

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.