Data Processing Addendum

This Data Processing Addendum (hereinafter referred to as "**Data Processing Addendum**") is by and between you ("**Customer**", "**you**", "**Controller**") and Howden Group Limited, or, if the Howden Uptime™ Solution License purchase was made in a country specified on the Howden Affiliate List document, the Howden Affiliate specified in such document (as applicable, "**HOWDEN**", "**Processor**") each a "**Party**" and collectively referred to as the "**Parties**".

PREAMBLE

(A) Processor performs monitoring services regarding rotating and non-rotating equipment for Controller. In order to access and review the monitoring services, Processor provides Controller with user accounts ("**Services**") as agreed between the Parties in the relevant Howden Uptime™ Solution License Agreement between Controller and Processor dated in accordance with DocuSign date noted therein, notwithstanding any dates of signing thereof or hereof, ("**Services Agreement**").

(B) In the course of providing the Services, Processor will process personal data within the meaning of Art. 4 no 1 of the EU General Data Protection Regulation ("**EU GDPR**") for which Controller or Controller's affiliates, (hereinafter referred to as "**Controller's Affiliates**"), are responsible as provided under Art. 4 no 7 EU GDPR ("**Controller's Personal Data**").

(C) This Data Processing Addendum regulates the data protection obligations of the Parties in regard to the processing of Controller's Personal Data under the Services Agreement and will reasonably ensure that such processing will only be rendered on behalf and under the Instructions of Controller, also on behalf of Controller's Affiliates, and to the extent the EU GDPR applies, in accordance with the EU GDPR, especially Art. 28 EU GDPR and, where applicable, the EU Standard Contractual Clauses for Processors (notified under document C (2010)593) ("**SCC**"), as contained in **Exhibit C** and to the extent the UK GDPR applies, the UK Addendum contained at **Exhibit D**, together with the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

(D) The Parties expressly consent to the processing of Controller Personal Data, and any personal data shared under and in connection with this Data Processing Addendum between the Parties, for the sole purposes of executing and performing their obligations under and in connection with the Services Agreement and as set out herein.

1. DEFINITIONS

1.1 "**Applicable Law**" means all laws, rules and regulations applicable to either Party's performance under this Data Processing Addendum, including but not limited to those applicable to the processing of personal data. This means in particular the UK GDPR, EU GDPR and all national laws validly amending the applicable rules for the processing of personal data.

1.2 "**Instruction**" means any documented instruction, submitted by Controller to Processor, directing Processor to perform a specific action with regard to personal data. Instructions shall initially be specified in the Services Agreement and may, from time to time thereafter, be amended, supplemented or replaced by Controller by separate text form (which includes letter, fax or e-mail) Instructions provided that such instructions still fall within the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the Applicable Law such as rectification, erasure, restriction or portability of personal data fall within the scope of the Services.

1.3 "**UK GDPR**" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.4 Terms used but not defined in this Section, including but not limited to "personal data", "personal data breach", "processing", "controller", "processor" and "data subject", will have the same meaning as set forth in Art. 4 EU GDPR.

2. AMENDMENT OF THE SERVICES AGREEMENT

2.1 Processor will, in the course of providing Services due under the Services Agreement, process Controller's Personal Data which shall be subject to the following provisions contained in this Data Processing Addendum.

2.2 This Data Processing Addendum amends the Services Agreement with respect to any processing of personal data by Processor as a processor for Controller pursuant to Art 4 No. 8 EU GDPR.

2.3 Controller enters into this Data Processing Addendum on its own behalf and on behalf of each of Controller's Affiliates and confirms being authorized to do so. Alternatively, Controller's Affiliates can co-sign this Data Processing Addendum.

2.4 When performing the Services, Processor will act either as processor or sub-processor. Processor's function as processor or sub-processor will be determined by the function of Controller and Controller's Affiliates. If Controller is the data controller, then Processor shall be the processor. If Controller is processor on behalf of Controller's Affiliates, then Processor shall be the sub-processor and Controller and any of Controller's Affiliates shall be entitled to issue Instructions under this Data Processing Addendum. The Parties agree that all Instructions and other communication of Controller's Affiliates to Processor will be passed on through Controller. In accordance with Section 6.2 Controller shall appoint a common point of contact which shall be authorized to issue all communication from Controller and Controller's Affiliates to Processor and receive all communication of the Processor to Controller and Controller's Affiliates.

2.5 In the following, unless expressly provided otherwise, a reference to Controller shall include a reference to Controller's Affiliates.

3. STANDARD CONTRACTUAL CLAUSES

3.1 If Controller or a Controller's Affiliate is located in the European Union or United Kingdom, any processing operation provided in the context of providing the Services shall not only be subject

to this Data Processing Addendum, but also to the SCC as contained in **Exhibit C**. The SCC shall prevail over any conflicting clauses in the Services Agreement or this Data Processing Addendum.

3.2 The Parties agree that the SCC shall be directly binding between Processor as data importer (as defined therein), Controller and/or each Controller's Affiliate located outside of the European Union as data exporter (as defined therein), in relation to that Controller's or Controller's Affiliate's Personal Data. Information to be provided according to Appendix 1 SCC shall be included by reference to the Preamble, Sec. 4.1 through 4.2 and the Services Agreement. Exhibit A of this Data Processing Addendum shall serve as Appendix 2 SCC. Sec. 8.2 and 8.3 shall apply respectively to the SCC. Reference in the SCC to the outdated EU Data Protection Directive (95/46/EC) shall be understood as a reference to the definitions in the EU GDPR. Where the scope of the definitions in Art. 4 EU GDPR go beyond what is defined in the SCC, the broader understanding shall apply.

4. SUBJECT, DURATION, PURPOSE, AND SPECIFICATION OF PROCESSING

4.1 The subject matter, nature and purpose of the processing are described in the Services Agreement and this Sec. 4.

4.2 The following types of personal data and categories of data subjects may be affected by the processing:

- *Categories of data subjects*: Employees, contractors, agents etc. of Controller or Controller's Affiliates and the employees of Controller's or Affiliate's contractors, agents, etc.
- *Types of personal data*: User account information, in particular: name, business email address, business mobile number, job title, information on access rights (specification of the rotating equipment accessible via the dashboard), password, documents stored in user account, sub user accounts created by user, alerts sent, information on use of account.
- *Special categories of personal data*: None.

4.3 The duration of the processing shall correspond to the duration of this Data Processing Addendum as set forth in Sec. 10.

5. PROCESSOR'S OBLIGATIONS

5.1 Processor shall in the course of providing Services, including with regard to transfers of personal data to a third country, process Controller's Personal Data only on behalf of and under the documented Instructions of Controller unless required to do so otherwise by Applicable Law; in such a case, Processor shall inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5.2 Processor shall take steps reasonably necessary to ensure that any natural person acting under its authority who has access to personal data does not process any personal data except

on Instructions from Controller, unless Processor, or he, she is otherwise required to do so by Applicable Law.

5.3 Processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this Data Processing Addendum.

5.4 Technical and Organizational Data Security Measures

5.4.1 The technical and organizational data security measures specified in **Exhibit A** are subject to technical advancements and development.

5.4.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 EU GDPR. As appropriate, this may include:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

5.4.3 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

5.4.4 If Processor significantly modifies measures specified in **Exhibit A**, such modifications have to meet the obligations pursuant to Sec. 5.4.2 and 5.4.3. Processor shall make available to Controller a description of such measures which enables Controller to assess compliance with Art. 32 EU GDPR. Processor and Controller shall agree on such significant modifications by signing the modified **Exhibit A** after every amendment. Controller shall not refuse to accept any modification that meets the requirements pursuant to Sec. 5.4.2 and 5.4.3.

5.4.5 Processor shall implement a data protection management procedure according to Art. 32 para 1 lit. d) EU GDPR, for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to reasonably ensure the security of the processing. Processor will further, by way of regular self-audits, reasonably ensure that the processing of Controller's Personal Data conforms with the provisions as agreed with Controller or with Controller's Instructions.

5.5 Processor shall, while taking into account the nature of the processing, assist Controller through appropriate technical and organizational measures, with the fulfilment of Controller's

obligations to respond to requests for exercising rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 EU GDPR.

5.6 Taking into account the nature of the processing and the information available to Processor, Processor shall assist Controller with ensuring compliance with the obligations pursuant to Art. 33 through 36 EU GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

5.7 Documentation and Audit Rights

5.7.1 Processor shall, upon request and subject to a non-disclosure agreement, provide to Controller a comprehensive documentation of the technical and organizational data security measures in accordance with industry standards.

5.7.2 If Controller has justifiable reason to believe that Processor is not complying with the terms and conditions under this Data Processing Addendum, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year (unless there are specific indications that require a more frequent inspection), Controller is, subject to a non-disclosure agreement, entitled to audit Processor. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Controller's Personal Data or (iii) by inspecting Processor's working premises whereby in each case no access to personal data of other customers or Processors' confidential information will be granted. Alternatively, Controller may also engage third party auditors to perform such tasks on its behalf in accordance with Sec. 5.7.4. The costs associated with such audits and/or for providing additional information shall be borne by Controller unless such audit reveals Processor's material breach with this Data Processing Addendum or Applicable Law.

5.7.3 If Controller intends to conduct an audit at Processor's working premises, Controller shall give reasonable notice to Processor and agree with Processor on the time and duration of the audit. In the case of a special legitimate interest, such audit can also be conducted without prior notice. Inspections shall be made during regular business hours and in such a way that business operations are not disturbed. At least one employee of Processor may accompany the auditors at any time. Processor may memorialize the results of the audit in writing which shall be confirmed by Controller.

5.7.4 Controller may not appoint a third party as auditor who (i) Processor reasonably considers to be in a competitive relationship to Processor or (ii) is not sufficiently qualified to conduct such an audit, or (iii) is not independent. Any such third-party auditor shall only be engaged if the auditor is bound by a non-disclosure agreement in favor of Processor prior to conducting any audit or is bound by statutory confidentiality obligations.

5.8 Notification Duties

5.8.1 Processor shall inform Controller without undue delay in text form (e.g. letter, fax or e-mail) of the following events:

- Requests from third parties including such from a data protection supervisory authority regarding Controller's Personal Data;
- Threats to Controller's Personal Data in possession of Processor by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, Processor shall immediately inform the respective responsible person/entity that Controller holds the sovereignty and ownership of the personal data.

5.8.2 For the purpose of enabling Controller to comply with its own data breach notification obligations pursuant to Art. 33 para 1 and Art. 34 para 1 EU GDPR, Processor shall notify Controller without undue delay after becoming aware of a personal data breach. Such notice will, if possible, include the following information:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; and
- a description of the measures taken or proposed to be taken by Processor and/or Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.8.3 Processor shall inform Controller immediately if, from its point of view, an Instruction of Controller may lead to a violation of Applicable Law. Until Controller either confirms or alternates the Instruction, Processor may refuse to comply with the Instruction issued.

5.9 Rectification, Erasure (Deletion), Restriction

5.9.1 If legally required and Controller is unable to perform the applicable task itself, or if provided so in the services description contained in the Services Agreement, Processor shall rectify, erase (delete), restrict (block) or transmit Controller's Personal Data upon Controller's request. Any erasure of Controller's Personal Data pursuant to this Sec. 5.9 shall be executed in such a manner that restoring or recovering such data is rendered reasonably impossible.

5.9.2 Unless Applicable Law requires a retention of the personal data, Processor shall, upon completion of the Services in consultation with Controller, either delete or return all Controller's Personal Data in its possession to Controller. In the case that statutory retention periods apply, Processor shall, upon expiry of such retention period immediately delete the retained Controller's Personal Data.

5.9.3 If a data subject addresses Processor with claims for access, rectification, erasure, restriction, objection or data portability, Processor shall refer the data subject to Controller.

5.10 Processor will inform Controller of the name and the official contact details of its data protection officer if Processor is, by Applicable Law, required to appoint a data protection officer. If Processor is not required to appoint a data protection officer, Processor shall – in its own discretion – name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this Data Processing Addendum.

5.11 In the case claims based on Art. 82 EU GDPR are raised against Controller, Processor shall reasonably support Controller with its defense to the extent the claim arises in connection with the processing of personal data by Processor in connection with performing the Services to Controller.

5.12 Processor will make available to Controller all information necessary to demonstrate compliance with the obligations laid down in this Data Processing Addendum and Art. 28 EU GDPR.

5.13 Processor will on request make available to a supervisory authority records of its processing activities based on Art. 30 EU GDPR.

5.14 Unless otherwise described in **Exhibit B** for the subprocessors, any data processing by the Processor shall take place within the European Economic Area.

6. CONTROLLER'S OBLIGATIONS

6.1 Controller shall provide all Instructions pursuant to this Data Processing Addendum to Processor in written, electronic or verbal form. Verbal Instructions shall be confirmed by Controller immediately in written form thereafter.

6.2 Controller shall notify Processor in writing of the names of the persons who are entitled to issue Instructions to Processor. Any consequential costs incurred resulting from Controller’s failure to comply with the preceding sentence shall be borne by Controller. In any event, the managing directors and personnel/human resource management of Controller are entitled to issue Instructions.

6.3 Controller shall inform Processor immediately if processing by Processor might lead to a violation of data protection regulations.

6.4 If claims based on Art. 82 EU GDPR are raised against Processor, Controller shall reasonably support Processor with its defense to the extent the claim arises in connection with the processing of personal data by Processor in connection with performing the Services to Controller.

7. SUBPROCESSING

7.1 Any subprocessor is obliged before initiating the processing, to commit itself in writing for the benefit of Controller and Controller's Affiliates to comply with the same data protection obligations as the ones under this Data Processing Addendum or legal Act within the meaning of Art. 28 para 3, 4 and 6 EU GDPR vis-à-vis Controller unless explicitly agreed otherwise. Any subprocessor must, in particular, agree to comply with the agreed technical and organizational

security measures in accordance with Sec. 5.4 herein and provide Processor with a list of the implemented technical and organizational measures. Subprocessor's measures may differ from the ones agreed between Controller and Processor but shall not fall below the level of data security as provided by the measures of Processor.

7.2 Where the subprocessor fails to fulfil its data protection obligations, Processor shall remain fully liable to Controller for the performance of the subprocessor's obligations.

7.3 Where a subprocessor refuses to be bound by the same data protection obligations as the ones under this Data Processing Addendum, Controller may consent to an alternative whereby such consent shall not be unreasonably withheld.

7.4 In the case a subprocessor is located outside the European Union/European Economic Area and not in a country/territory which, pursuant to Art. 45 EU GDPR, provides for an adequate level of data protection, Processor shall conclude a data processing agreement based on the SCC with that subprocessor. Processor shall also be entitled to conclude SCC or any other standard protection clauses in the name and for the benefit of Controller. Controller herewith authorizes Processor to conclude such agreement in its own name.

7.5 Controller herewith agrees also on behalf of Controller's Affiliates to the subprocessors as set out in **Exhibit B**.

8. LIABILITY

8.1 Controller and Processor shall be each liable for damages of concerned data subjects according to Art. 82 EU GDPR (external liability).

8.2 Either Party shall be entitled to claim back from the other, Processor or Controller, that part of the compensation, corresponding to their part of responsibility for the damage (internal liability).

8.3 As regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, Processor’s liability for breach of any terms and conditions under these Terms of Data Processing shall be subject to the liability limitations agreed in the Services Agreement. Further, no Controller's Affiliate shall become beneficiary of this Data Processing Addendum without being bound by this Data Processing Addendum and without accepting this liability limitation. Controller will indemnify Processor against any losses that exceed the liability limitations in the Services Agreement suffered by Processor also in connection with any claims of Controller's Affiliates or data subjects based on alleged violation of this Data Processing Addendum.

9. COSTS FOR ADDITIONAL SERVICES

If Controller's Instructions lead to a change from or increase of the agreed Services or in the case of Processor's compliance with its obligations pursuant to Sec. 5.6, 5.9 or 5.11 to assist Controller with Controller's own statutory obligations, Processor is entitled to charge reasonable fees for such tasks

which are based on the prices agreed for rendering the Services and/or notified to Controller in advance.

10. CONTRACT PERIOD

The duration of this Data Processing Addendum coincides with the duration of the Services Agreement. It commences and terminates with the provision of the Services under the Services Agreement, unless otherwise stipulated in the provisions of this Data Processing Addendum. Provisions, which, by their nature, survive the duration of this Data Processing Addendum, remain in force.

11. MODIFICATIONS

The Parties may modify or supplement this Data Processing Addendum, with notice to Controller, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the EU GDPR. Controller shall notify Processor if it does not agree to a modification, in which case Processor may terminate the Data Processing Addendum with two (2) weeks' prior written notice, whereby in the case of an objection not based on incompliance of the modifications with applicable data protection law, Processor shall remain entitled to claim its agreed remuneration until the term end.

12. WRITTEN FORM

Any side agreements to this Data Processing Addendum as well as changes and amendments of this Data Processing Addendum or the Services hereunder, including this Sec. 12, shall be in writing.

13. CHOICE OF LAW

This Data Processing Addendum is governed by, and shall be interpreted in accordance with, the law of England & Wales, excluding its conflict of law provisions. The place of jurisdiction for the resolution of any disputes arising from or under this Data Processing Addendum shall be England & Wales.

14. MISCELLANEOUS

14.1 With respect to any issues arising out of or in connection with the processing of personal data, this Data Processing Addendum shall prevail over all other agreements between the Parties, except the SCC.

14.2 This Data Processing Addendum may only be amended, supplemented or changed upon the written agreement of the Parties.

14.3 In the event a clause under the Services Agreement has been found to violate the EU GDPR, UK GDPR or any other Applicable Laws, the Parties will mutually agree on modifications to the Services Agreement to the extent necessary to ensure data privacy-law compliant processing.

EXHIBIT A

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Art. 32 EU GDPR:

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by Data Importer. If so requested, data importer will provide data exporter with a description of the then current measures.

1. Pseudonymization and Encryption, Art. 32 para 1 point a EU GDPR

Pseudonymization contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Stored personal data is limited to name, company email address, job title and location.
- Stored data, including back-ups, is encrypted where appropriate.

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, Art. 32 para 1 point b EU GDPR

Confidentiality and integrity is ensured by the secure processing of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

2.1 Confidentiality

2.1.1. Physical access control

Measures that prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- HOWDEN's third party provider, Microsoft, takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources.
- Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:
    - Access request and approval. Visitors must request access prior to arriving at the datacenter. Visitors are required to provide a valid business justification for their visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the

datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

  - Facility's perimeter. When arriving at a datacenter, visitors are required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.

  - Building entrance. The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.

  - Inside the building. After entering the building, visitors must pass two-factor authentication with biometrics to continue moving through the datacenter. If their identity is validated, they can enter only the portion of the datacenter that they have approved access to. They can stay there only for the duration of the time approved.

  - Datacenter floor. Visitors are only allowed onto the floor that they are approved to enter. They are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When visitors exit the datacenter floor, they again must pass through full body metal detection screening. To leave the datacenter, one is required to pass through an additional security scan.

  - Microsoft requires visitors to surrender badges upon departure from any Microsoft facility.

- Physical security reviews

  - Periodically, Microsoft conduct physical security reviews of the facilities, to ensure the datacenters properly address Azure security requirements. The datacenter hosting provider personnel do not provide Azure service management. Personnel are unable to sign in to Azure systems and do not have physical access to the Azure collocation room and cages.

- Data bearing devices

  - Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that cannot be wiped, a destruction process is used that destroys it and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. The means of disposal is determined according to the asset type and records of the destruction are retained.

- Equipment disposal

- Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing the data is not made available to untrusted parties. A secure erase approach is used for hard drives that support it. For hard drives that cannot be wiped, a destruction process is used that destroys the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. The means of disposal is determined according to the asset type. Records of the destruction are retained. All Azure services use approved media storage and disposal management services.

- Compliance

    - Microsoft design and manage the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. They also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

- Testing

    - Penetration testing is carried out on a periodic basis and the results of these tests can be made available upon request after completion of a non-disclosure agreement.

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorization.

- User Authentication by simple authentication methods (using username/password).
- Secure transmission of credentials using networks (using TSL, SSL and Private APN).
- Guidelines for handling of passwords and password requirements.
- Access control to infrastructure that is hosted by cloud service provider.

2.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

- Access right management including authorization concept, implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.
- Access right management linked to a user’s organization and area of responsibility.
- Customer access right management for their organization only.

2.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Personal data is only collected for the purpose of access to the Howden Uptime system.
- Data separation. Data streams are stored using a unique tag basis and each is tied to a unique asset. Individual data streams can be selected, extracted and deleted as required as can entire asset data sets.

2.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding to the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff.

2.2. Integrity

2.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, 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.

- Secure transmission between Edge device and server by using industry-standard encryption and a private APN.
- Regular rotation of encryption keys and the maintenance of an electronic safe list.
- Secure network interconnections ensured by Firewalls etc.
- Logging of transmissions of data from IT system that stores or processes personal data.
- Secure transmission between server and web browser by using industry-standard encryption.
- Audit logging of data transmissions.

2.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Data can only be input by a limited number of authorized users.
- All users must sign in using logging authentication and user system access is also monitored.
- User data input, user data change and user data deletion is logged by the platform.

2.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes

measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- As the Howden Uptime model server is hosted in the Microsoft Azure cloud, the environment is backed up once a day.
- The data repository, containing process data and user data is continually backed up and can be restored to any single point in time using the Azure Backup service.

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, Art. 32 para 1 point c EU GDPR

Organizational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- Back up capabilities are as per section 2.3 of this Exhibit A.
- Back-ups are kept for a minimum period of six (6) months.
- In the event of a physical or technical incident a response to a personal data enquiry will be provided within twenty-four (24) hours. Access to the data will be made available in a reasonable timescale depending on the size of the data repository to be restored.

4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing, Art. 32 para 1 point d EU GDPR

Organizational measures that ensure the regular review and assessment of technical and organizational measures.

- A limited number of people have access to the data repository.
- All users with access are named and authenticated.
- All users have completed annual training in GDPR and Information Security Awareness.

EXHIBIT B

SUBPROCESSORS

Name	Address	Description of Processing	Location of Processing
PTC	PTC Corporate Headquarters, 140 Kendrick Street, Needham, MA 02494, United States of America	Howden Uptime is configured using the PTC Thingworx suite of products and PTC's Kepware product is used on the Edge device.	USA
Microsoft	Microsoft Corporation Headquarters, One Microsoft Way, Redmond, WA 98052, United States of America	Microsoft Azure cloud services is used to host the Howden Uptime model and the data repository.	USA
AT&T	AT&T Corporate Headquarters, 208 South Akard Street, Dallas, TX 75202, United States of America	AT&T provide the private cellular network to transmit the data from the Edge device to the Microsoft Azure cloud.	USA
InVMA	Coney Green Business Centre, Claycross, Chesterfield, Derbyshire, S45 9JW, United Kingdom	Systems integrator and UK re-seller of the PTC Thingworx product. Used for platform configuration.	United Kingdom
Howden Group Limited	1 Chamberlain Square Cs, Birmingham, United Kingdom, B3 3AX	Creation and management of Howden Uptime user account information.	United Kingdom

EXHIBIT C

STANDARD CONTRACTUAL CLAUSES FOR 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.

Controller and/or each of the Controller's Affiliates is hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by the respective Data Exporter.

Processor is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a “party” and collectively “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;

(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;

(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 or United Kingdom jurisdiction in which the Data Exporter is established;

(f) *'Technical and Organizational Security Measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 Organizational 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, unauthorized 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

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 Organizational 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 unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 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 Applicable Data Protection Law.

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 (This requirement may be satisfied by the Subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). 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.

APPENDIX 1

For information required under Appendix 1 SCC, please see Preamble and Sec. 4.1 through 4.2 of the Data Processing Addendum.

APPENDIX 2

For information required under Appendix 2 SCC, please see Exhibit A of the Data Processing Addendum.

EXHIBIT D
UK ADDENDUM

This Addendum 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.

This International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (hereinafter "**UK Addendum**") is entered into by and between Howden Group Limited and Customer as of and effective beginning on the date of the Services Agreement agreed between the Parties. During the course of providing Services to, or on behalf of, Howden Group Limited together with its Affiliates ("**HGL**") pursuant to the Services Agreement between HGL and Customer (the "**Agreement**"), Customer may access or otherwise process personal data. The Parties agree that with regard to the processing of personal data pursuant to the Agreement or this UK Addendum, HGL is the data processor (and shall hereinafter be referred to as the "**Data Receiver**"), Customer is the data discloser (and shall hereinafter be referred to as the "**Data Discloser**") and the parties are independent controllers.

The Parties have agreed that the Data Receiver will provide the Services to the Data Discloser pursuant to and in accordance with the terms and conditions of this UK Addendum. In the event of a conflict between the terms of this UK Addendum and the Agreement, to which this UK Addendum applies, the terms of this UK Addendum shall govern as far as in accordance with applicable laws.

Part 1: Tables

Table 1: Parties

Start date	[ ]	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: [ ] Trading name (if different): [ ] Main address (if a company registered address): [ ]	Full legal name: [ ] Trading name (if different): [ ] Main address (if a company registered address): [ ]

	Official registration number (if any) (company number or similar identifier): [ ]	Official registration number (if any) (company number or similar identifier): [ ]
Key Contact	Full Name (optional): [ ] Job Title: [ ] Contact details including email: [ ]	Full Name (optional): [ ] Job Title: [ ] Contact details including email: [ ]
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: [ ] Reference (if any): [ ] Other identifier (if any): [ ] Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Table 4: Ending this Addendum when the Approved Addendum Changes

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- Sections **Error! Reference source not found.** to **Error! Reference source not found.** override Clause 5 (Hierarchy) of the Addendum EU SCCs;
- and this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.
The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:
References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
In Clause 2, delete the words:

- "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

- 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.";

- Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

- Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

- References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

- References to Regulation (EU) 2018/1725 are removed;

- References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

- The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

- Clause 13(a) and Part C of Annex I are not used;

- The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

- In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

- Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

- Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

- The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

- makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in: its direct costs of performing its obligations under the Addendum; and/or its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.