EXHIBIT A

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") is executed between **Hillenbrand, Inc.** ("Hillenbrand" on behalf of itself and its affiliates (acting as the controller or CCPA-covered business)), and [VENDOR], ("Vendor" (acting as the processor or service provider)). Hillenbrand and Vendor are hereinafter referred to jointly as the "Parties" and each individually as a "Party."

BACKGROUNND:

Hillenbrand and Vendor are entering into this DPA further to the Master Services Agreement between Hillenbrand and Vendor, effective as of **[insert date]** (the "Agreement") relevant to Vendor's provision of the Services. The Parties have agreed to enter into this DPA for purposes of compliance with Applicable Data Protection Law.

The DPA shall form an integral part of the Agreement. References in this DPA are to the Agreement as amended by this DPA.

In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement, the order of priority shall be as follows: (a) the Standard Contractual Clauses, where applicable; (b) this DPA; (c) any other personal information or data processing agreements or obligations between the Parties; and (d) the Agreement. Capitalized terms not defined herein shall have the meanings given to them in the Agreement.

The DPA is effective as of **[insert date]** or the effective date of the Agreement (the "Effective Date"), whichever is earlier.

AGREED TERMS:

1. **Definitions.** The following definitions shall apply for this DPA:

"Business", **"business purpose"**, **"consumer"**, **"personal information"**, **"sell"**, **"sale"**, and **"service provider"** shall have the meanings given to such terms in the CCPA. Personal information includes all personal information subject to applicable Data Protection Law that Vendor may process on Hillenbrand's behalf.

"**CCPA**" means the California Consumer Privacy Act of 2018, and any regulations promulgated thereunder, each as amended from time to time.

"Consumer", **"data processor"** or **"processor"**, **"data controller"** or **"controller"**, **"data subject"**, **"personal data"**, **"personal data breach"**, **"processing"**, **"recipient"** and **"supervisory authority"** shall have the meanings given to such terms in the GDPR or other Data Protection Law.

"**Consumer Rights Request**" means a communication from a consumer regarding the exercise of rights provided by the CCPA, the CPRA or other applicable U.S. Data Protection Law, including but not limited to rights to request to know and delete personal information.

"CPRA" means the California Privacy Rights Act of 2020, and any regulations promulgated thereunder, each as amended from time to time.

"CSL" means the Cybersecurity Law of the People's Republic of China of 2016, and any regulations promulgated thereunder, each as amended from time to time.

"DSL" means the Data Security Law of the People's Republic of China of 2021, and any regulations promulgated thereunder, each as amended from time to time.

"Data Protection Law" means all applicable international, U.S. federal, U.S. state, and local security, confidentiality, and/or privacy laws, standards, guidelines, policies, regulations, and procedures that are applicable to Hillenbrand, Vendor, the Services, and/or any other programs or products provided pursuant to the Agreement. Data Protection Law includes but is not limited to the CCPA; the CPRA; the GDPR and any European Economic Area ("EEA") Member State data protection laws or regulations implementing or supplementing the GDPR; the UK Data Protection Act 2018 and any national legislation that amends, re-enacts, replaces or supplements data protection laws in the United Kingdom that arises from the withdrawal of the United Kingdom from the European Union including The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, in particular the UK GDPR (all together "UK Data Protection Laws"); the Swiss Federal Act on Data Protection ("FADP") the Swiss Federal Act on Data Protection ("FADP"); and the CSL, DSL and PIPL, to the extent such laws apply to the Services, each as amended from time to time.

"Data Subject Request" means a communication from a data subject regarding the exercise of rights pursuant to Data Protection Law, including rights to access, rectification, restriction of processing, erasure, and portability of personal data, as applicable.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 and any member state implementing regulations, each as amended from time to time.

"Information Security Incident" means any actual or suspected personal data breach of any Hillenbrand personal data processed by Vendor or Subprocessor, or security breach, or other unauthorised access, or disclosure, misappropriation, loss, damage, or other compromise of the security, confidentiality, or integrity of any Hillenbrand personal data or personal information processed by Vendor or a Subprocessor.

"Standard Contractual Clauses (SCCs)" means, as applicable, the Standard Contractual Clauses (aka Model Clauses) for the transfer of personal data to processors established in third countries (i) as approved by the European Commission Decision of 4 June 2021, and (ii) the SCCs as approved by the European Commission Decision of 4 June 2021 but modified for application in the UK by the addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (iii) as adopted by the Federal Data Protection and Information Commissioner (Switzerland) on August 27, 2021, each as amended, from time to time and as further detailed in Attachment A to this DPA.

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly with a particular individual, in whatever format, including information contained in communications, documents, databases, records or materials of any kind whether in individual or aggregate form.

"Personal data" shall have the meaning given to such term in the GDPR and for purposes of this DPA, includes personal information and all personal data subject to applicable Data Protection Law that Vendor may process on Hillenbrand's behalf.

"PIPL" means the Personal Information Protection Law of the People's Republic of China of 2021, and any regulations promulgated thereunder, each as amended from time to time.

"Services" means the services and other activities that Vendor shall provide or carry out for Hillenbrand as set forth in the Agreement.

"Subprocessor" means any subcontractor engaged by Vendor for the provision of the Services that will process Personal Data or Personal Information provided by Hillenbrand.

2. Scope and Operation.

2.1 This DPA applies to i) Vendor's processing of personal data to the extent that it is subject to GDPR Article 28, or UK GDPR Article 28, or FADP Section 9 and ii) Vendor's processing of personal information that is subject to Data Protection Law in providing Services to Hillenbrand in accordance with the Agreement.

2.2 As required by Article 28(3) of the GDPR, the subject-matter and duration, nature, and purpose of the processing; type of personal data; and the categories of data subjects, and the obligations and rights of the controller(s) associated with Vendor's processing of personal data in the provision of the Services as well as the applied technical and organizational measures and Subprocessors engaged are set forth in, and in accordance with, the Agreement and **Attachment B** to this DPA.

2.3 The duration of the processing is the term of the Agreement and until all Hillenbrand personal data has been deleted or returned by Vendor in accordance with Section 10 and, as applicable, the SCCs to this DPA.

3. Relationship of the Parties.

3.1 The Parties agree that with respect to the provision of the Services, Hillenbrand is the data controller of the personal data and/or a business with respect to personal information and Vendor is the data processor of such personal data and/or a service provider with respect to such personal information. The Vendor confirms that it shall not sell personal information and/or combine personal information from different sources. To the extent that the personal information is subject to the CCPA or CPRA, Vendor (i) is engaged in such processing on behalf of Hillenbrand and is receiving and processing Hillenbrand's personal information in furtherance of one or more enumerated business purposes under the CCPA; (ii) shall not sell personal information; and for the purposes of CPRA compliance, (iii) shall not combine personal information from different sources. Vendor understands the restrictions explicitly set forth in the CCPA or CPRA, as applicable, and certifies that it will comply with such restrictions.

3.2 In accordance with GDPR Article 28(3)(a) and any other Data Protection Law, Vendor and any Subprocessor shall only process personal data and/or personal information as set forth in the Agreement or other documented instruction given by Hillenbrand, unless otherwise required by law to which Vendor is subject, including but not limited to, European Union or EEA Member State law and/or U.S. state and federal law. In this case, Vendor shall inform Hillenbrand of the relevant legal requirement prior to such processing, unless Vendor is legally prohibited from informing Hillenbrand of the requirement.

4. Security Measures. In performing the Services, Vendor shall:

4.1 implement, maintain and monitor a comprehensive written information security program that contains appropriate administrative, technical, and organizational measures to ensure the security and confidentiality of Hillenbrand personal data/personal information and to prevent unauthorized or unlawful processing of personal data/personal information and any loss, destruction of, or damage to personal data/personal information ("Information Security Program"). The safeguards will be appropriate to the risk associated with the processing activity, including, at a minimum, the measures referred to in GDPR Article 32(1);

4.2 implement appropriate security measures that meet or exceed prevailing industry standards and are in accordance with the requirements of the GDPR and any other Data Protection Law;

4.3 regularly test, assess, and evaluate the effectiveness of the Information Security Program for ensuring the secure processing of personal data/personal information and regularly monitor compliance with such security safeguards and ensure that there is no material decrease in the level of security afforded to Hillenbrand personal data and/or personal information during the duration of the processing, and

4.4 at minimum, apply the technical and organizational measures described in **Annex II** to **Attachment B** of this DPA.

5. Confidentiality and Restrictions on Use.

5.1 Vendor shall treat all personal data and/or personal information processed on behalf of Hillenbrand in accordance with the Agreement as confidential information.

5.2 Vendor shall not retain, use, or disclose the personal data/personal information it receives from Hillenbrand for any purpose other than performing the Services for Hillenbrand as specified in the

Agreement. Vendor shall not sell the personal data/personal information it receives from Hillenbrand, nor shall it retain, use, or disclose such personal data/personal information outside of its direct business relationship with Hillenbrand. Vendor certifies that it understands the restrictions outlined in this section and will comply with them.

5.3 Vendor shall ensure that persons authorized to process Hillenbrand personal data and/or personal information have been informed of their responsibilities and have executed written confidentiality agreements or are otherwise subject to confidentiality obligations. Vendor shall ensure that such commitments to confidentiality endure through the duration of the processing and after termination or conclusion of processing. Vendor shall also treat this DPA as confidential information.

5.4 Vendor shall limit access to Hillenbrand personal data and/or personal information to Vendor's personnel and any Subprocessor's personnel that requires such access in order to perform the Services. Any such access to Hillenbrand personal data and/or personal information shall be granted on a strict need-to-know basis.

6. Subprocessing.

6.1 Vendor shall not engage any Subprocessor or disclose any personal data and/or any personal information to any outside entity without Hillenbrand's prior specific written consent, and without Hillenbrand's prior specific written consent, and only for the purpose of performing the Services specified in the Agreement or as otherwise permitted by Data Protection Law. Vendor shall inform Hillenbrand in writing, through the email addresses of its then-current, active points of contact at Hillenbrand, at least one month in advance of its intention to add or replace a Subprocessor. Such notification shall include the identity of such Subprocessor, the location in which Hillenbrand personal data and/or personal information would be processed by such Subprocessor, and a description of the relevant processing activities to be carried out by the Subprocessor.

6.2 Vendor shall ensure that Subprocessors are bound by a written agreement requiring such Subprocessor to adhere to the same data protection obligations as those applicable to Vendor under this DPA, including a right for Hillenbrand to audit Subprocessor, and all requirements of Data Protection Law. Vendor shall respect the conditions imposed by GDPR Article 28(2) and (4) regarding the engagement of Subprocessors.

6.3 Vendor may continue to use Subprocessors engaged as of the Effective Date of this DPA, subject to compliance with Vendor's obligations under this DPA, the Agreement, and applicable Data Protection Law.

6.4 Vendor shall provide a list of its Subprocessors to Hillenbrand at any time upon request.

6.5 Vendor shall remain fully liable for any personal data and/or personal information processing, including any acts or omissions, by Vendor's Subprocessors.

7. Data Subject Requests and Consumer Rights Requests.

7.1 Vendor shall, without undue delay, and in any event within five (5) business days, notify Hillenbrand if it receives a Data Subject Request regarding Hillenbrand personal data or a Consumer Rights Request regarding Hillenbrand personal information. Vendor shall not respond to any Data Subject Request or Consumer Rights Request, unless and until expressly instructed to do so by Hillenbrand or unless required to respond by applicable law.

7.2 Vendor shall provide all reasonable assistance to Hillenbrand to ensure Hillenbrand is compliant with its obligation to respond to Data Subject Requests and/or Consumer Rights Requests under Data Protection Law and also to the extent required as per the terms and conditions of this DPA. If authorized by Hillenbrand, such assistance may include complying with a Data Subject Request and/or Consumer Rights Request in accordance with Data Protection Law and Hillenbrand instructions.

7.3 Vendor shall comply with any Data Subject Request and/or Consumer Rights Request regarding the deletion of an individual's personal data and/or personal information. Upon direction from

Hillenbrand to execute a deletion request, Vendor shall delete the personal data and/or personal information in question within 30 business days. If Vendor is unable to delete such personal data and/or personal information by the aforementioned deadline, it shall promptly notify Hillenbrand in writing.

7.4 If Hillenbrand requests information from Vendor to fulfill its obligation to respond to a Data Subject Request or Consumer Rights Request, Vendor shall provide the requested information without undue delay, and in any event within 72 hours of Hillenbrand's request for assistance. Vendor shall notify Hillenbrand immediately if Vendor is unable to comply with the request for assistance. Such notification shall provide a detailed explanation as to why Vendor considers compliance with such request for assistance to be impossible.

7.5 During the term of the Agreement, Vendor shall provide Hillenbrand with any personal data and/or personal information that it processes on Hillenbrand's behalf in a structured, commonly used, electronic, and machine-readable format or in such format as otherwise requested by Hillenbrand.

8. Information Security Incident.

8.1 Vendor shall notify Hillenbrand without undue delay, and at the latest within 24 hours after becoming aware of an Information Security Incident affecting Hillenbrand personal data and/or personal information. The notification, at a minimum, shall include: (i) a description of the Information Security Incident, including the number and categories of individuals concerned, the date and time of the relevant incident and the nature and content of the personal data and/or personal information affected; (ii) a description of the incident and the circumstances that led to the Information Security Incident (e.g., loss, theft, copying); (iii) a description of recommended measures to mitigate any adverse effects of the Information Security Incident; (iv) a description of the likely consequences and potential risk that the Information Security Incident may have towards affected individuals; (v) a description of the measures proposed or taken by Vendor to address the Information Security Incident; and (vi) any other information required by Data Protection Law.

8.2 In the event of an Information Security Incident, Vendor shall immediately take action to contain such Information Security Incident and mitigate potential risks to affected data subjects or consumers. Vendor shall assist Hillenbrand to investigate, remediate and take any other action Hillenbrand deems necessary regarding an Information Security Incident. Vendor shall provide all reasonable assistance to Hillenbrand to ensure Hillenbrand is compliant with its obligations regarding an Information Security Incident under Data Protection Law.

8.3 In the event of an Information Security Incident, Hillenbrand has the right to control the breach notification process, unless Data Protection Law dictates otherwise. Vendor shall not communicate with any outside entity (including any data subjects, consumers, law enforcement, supervisory authority or other government agency) regarding Hillenbrand in connection with any Information Security Incident, unless and until expressly instructed to do so by Hillenbrand.

8.4 In the event of an Information Security Incident, Vendor will be liable for any costs and expenses incurred by Hillenbrand in connection with the Information Security Incident, including those costs and expenses incurred in: (i) preparing and delivering notices to affected individuals; (ii) providing credit monitoring services or other credits or benefits extended to affected individuals to mitigate their risk of harm; (iii) preparing and mailing or other transmission of such other communications to affected individuals as Hillenbrand deems reasonably appropriate; (iv) establishing a call center or other communications procedures in response to an Information Security Incident; (v) reasonable attorneys' fees associated with investigating, remediating and responding to the Information Security Incident; (vi) engaging public relations and other similar crisis management services; (vii) retaining forensic investigators and accountants; (viii) any liability to third parties that Hillenbrand incurs in connection with the Information Security Incident (such as amounts paid or for which Company is liable to third parties in tort or arising out of contracts); and (ix) labor and subcontracting, including but not limited to employee time spent and additional service provider costs incurred in connection with the Information Security Incident.

9. Audits and Inspections.

9.1 Vendor shall make available to Hillenbrand any information Hillenbrand may require for purposes of demonstrating compliance with Hillenbrand's obligations under Data Protection Law.

9.2 Vendor shall allow for and contribute to audits conducted by Hillenbrand or another auditor instructed by Hillenbrand, provided that such auditor shall not be a direct competitor of Vendor. If Vendor believes any request for information or cooperation pursuant to Section 9 of this DPA may infringe applicable law, it shall immediately notify Hillenbrand in writing.

9.3 At least annually, Vendor shall supply its current and active Hillenbrand points of contact with a copy of its most recent internal or third-party audits and/or certifications, including any SOC-2, or any successor form of report, which will be subject to the confidentiality requirements in the Agreement.

10. Deletion or Return of Hillenbrand Personal Data and/or Personal Information.

10.1 Vendor shall, upon receipt of Hillenbrand's written request, securely delete or return Hillenbrand personal data and/or personal information to Hillenbrand and delete existing copies, unless EU law or EEA Member State law and/or U.S. state or federal law, respectively, requires storage of the personal data and/or personal information, or unless otherwise prohibited by applicable law.

10.2 Vendor shall return all Hillenbrand personal data and/or personal information in a commonly used, structured, electronic, and machine-readable format or in such format as otherwise requested by Hillenbrand.

10.3 Immediately after deleting the Hillenbrand personal data and/or personal information, Vendor shall provide to its current, active Hillenbrand points of contact certified written confirmation of such secure deletion.

11. Data Transfers.

11.1 Vendor shall not transfer or disclose Hillenbrand personal data to any recipient outside the EEA, Switzerland, or United Kingdom without the prior written permission of Hillenbrand unless the recipient is in a jurisdiction deemed to have adequate level of data protection by the EU Commission. For the avoidance of doubt: Section 6 of this DPA remains unaffected by the previous sentence. In the event that Vendor or any of Vendor's Subprocessors is a recipient of Hillenbrand personal data outside the EEA, Switzerland, United Kingdom, or outside any other jurisdiction deemed to have adequate level of data protection by the EU Commission, Vendor shall comply with the SCCs pursuant to **Attachment A** to this DPA. In the event of any inconsistency between this DPA and the SCCs, the SCCs shall govern.

11.2 Vendor shall not transfer Hillenbrand Personal Data outside of China unless such transfers comply with this DPA and **Annex II to Attachment B**; however, the SCCs shall not apply to such transfers.

11.3 In the event that any of the data transfer mechanisms set forth in Section 11 of this DPA are amended, replaced, or repealed by the European Commission, Court of European Justice, or under Data Protection Law, the Parties shall work together in good faith to enter into an updated version of such data transfer mechanism, provide assurances as required under Data Protection Law or to negotiate a solution to enable compliant transfers of personal data.

12. Data Protection Officer. The Vendor shall provide to Hillenbrand contact details of its Data Protection Officer, if applicable.

13. Claims; Inquiries from Law Enforcement, Government Agencies. Vendor shall promptly (i) communicate any request for information about Hillenbrand or its use of the Services from law enforcement, supervisory authority or other government agency, including a supervisory authority, unless Vendor is prohibited to do so by law; and (ii) if Hillenbrand faces an actual or potential claim arising out of or related to an alleged violation of any Data Protection Law, provide all materials and information requested by Hillenbrand that are relevant to the defense of such claim and the underlying circumstances concerning the claim.

14. **Insurance.** In addition to any other insurance required under the Agreement, Vendor shall maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for Information Security Incidents, privacy violations, and notification costs) of at least $10,000,000.00 U.S. per occurrence.

15. **Data Protection Impact Assessments**. Vendor shall provide all reasonable assistance to ensure Hillenbrand is compliant with its obligations in GDPR Article 35 and 36 related to conducting data protection impact assessments in relation to the Services and seeking prior consultation from supervisory authorities.

16. **Recordkeeping.** In accordance with the requirements of GDPR Article 30(2), Vendor shall maintain a record of all processing activities carried out on Hillenbrand's behalf. Vendor shall make such record available to Hillenbrand and the applicable supervisory authority upon request.

17. **Allocation of Costs.** Each Party shall perform its obligations under this DPA at its own cost, unless otherwise specified herein.

18. **Electronically Transmitted Documents and Signatures.** An electronic signature or a manual signature on this DPA, the image of which (in either case) is transmitted electronically, shall constitute an original signature for all purposes and the Parties shall not dispute the legally binding nature, validity, or enforceability of this DPA based on the fact that the terms were accepted with any such electronic or manual signature.

19. **Termination.** Any breach of this DPA by Vendor shall constitute a material breach of the Services Agreement that (i) gives rise to Hillenbrand's termination rights under the Agreement, and (ii) shall not be subject to any limitation or exclusion of liability provisions contained in the Agreement.

20. **Indemnity.** Vendor hereby agrees to indemnify and keep indemnified, hold harmless, and if instructed by Hillenbrand (at Hillenbrand's sole discretion), defend at its own expense, Hillenbrand and its subsidiaries and affiliates and their respective officers, directors, employees, personnel and other representatives from and against all claims, suits, hearings, actions, costs, damages, liabilities, penalties, judgments or expenses (including but not limited to legal fees, administrative penalties, investigation costs and legal costs (calculated on a full indemnity basis)) arising out of or relating to (i) Vendor's or its Subprocessor's violation of Data Protection Law, or (ii) Vendor's or its Subprocessor's breach of this DPA. These indemnification obligations apply in addition to, not in lieu of, any other Vendor indemnification obligations specified in the Services Agreement.

21. **Amendment.** Upon written agreement by both Parties, this DPA may be amended as necessary, including to comply with updates to any Data Protection Laws.

22. **Third-Party Beneficiaries.** The Parties agree that Hillenbrand's subsidiaries and affiliates that are receiving the Services from the Vendor are intended third-party beneficiaries of this DPA and this DPA is intended to relay the same benefits to Hillenbrand's subsidiaries and affiliates that are receiving the Services from the Vendor.

23. **New Privacy Laws.** The Parties understand that various countries, states and provinces are actively considering enacting other privacy laws which may conflict with, preempt and/or place additional regulations on current Data Protection Laws ("New Privacy Laws"). Vendor agrees that it will work in good faith with Hillenbrand to ensure any sharing of personal data and/or personal information between the Parties is done in compliance with New Privacy Laws. The Parties further agree that should any specific Data Protection Law be preempted, invalidated or cease to be effective, this DPA shall continue to survive with respect to each Party's rights and obligations under other Data Protection Laws.

IN WITNESS WHEREOF, Hillenbrand and Vendor have executed this DPA, which will come into force on the Effective Date.

Hillenbrand, Inc. **Defmacro Software Private Limited**

By: ____________________________________

By:____________________________________

Name: ____________________________________ Name: ____________________________________

Title: ____________________________________ Title: ____________________________________

Date: ____________________ Date: ____________________

ATTACHMENT A: STANDARD CONTRACTUAL CLAUSES

The SCCs shall apply as follows:

I. **EUROPEAN UNION (personal data subject to Art. 28 GDPR)**: For purposes of this Agreement, Hillenbrand and Vendor adopt module 2 (controller-to-processor) of the SCCs, which are hereby incorporated and completed as follows: the "data exporter" is each Hillenbrand affiliate having its registered place of business in the EEA and allowing data importer to process its personal data under Art. 28 GDPR; the "data importer" is Vendor; the optional docking clause in Clause 7 is implemented; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is excluded; Clause 13(a) paragraph 1 is implemented; Clause 17 option 1 is implemented and the governing law is the law of Germany; the court in Clause 18(b) are the Courts of Germany; Annex I, II and III to module 2 of the SCCs are Annex I, II and III of Attachment B to this DPA respectively.

II. **CHINA:** For the purposes of this Agreement, Vendor agrees to Processing Personal Data in a manner consistent with industry best practices and applicable laws and regulations, including in the manner set forth below. Vendor acknowledges and warrants that the protection measures for the Personal Data have met the requirements of applicable laws, regulations, policies and industry standards.

III. **SWITZERLAND (personal data subject to Sec. 9 FADP)**: For the purposes of this Agreement, the SCCs apply pursuant to Sec. I above with the following deviations:

- o ***Clause 13/Annex I C***, Supervisory Authority: Where the data subjects are in Switzerland, the Federal Data Protection and Information Commissioner.
- o ***Clause 17, Governing Law***: Where the data subjects are in Switzerland, the laws of Switzerland.
- o ***Clause 18, Forum and Jurisdiction***: Where the data subjects are in Switzerland, Switzerland.

IV. **UNITED KINGDOM (personal data subject to Art. 28 UK GDPR)**: For purposes of this Agreement, the SCCs apply as set forth for application in the UK by the addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, with the following details: (i) in Table 1, the "Exporter" is each Hillenbrand affiliate having its registered place of business in the UK and allowing Importer to process its personal data under Art. 28 GDPR, and the "Importer" is Vendor, their details are set forth in this DPA; (ii) in Table 2, the second option is selected and the "Approved EU SCCs" are the SCCs as applicable pursuant to Sec. I of this Attachment A above (iii) in Table 3, Annexes 1 (A and B), II, and III to the "Approved EU SCCs" are Annex I, II, and III of Attachment B to this DPA respectively; and (iv) in Table 4, neither the "Importer" nor the "Exporter" can terminate the SCCs.

V. **ATTACHMENT B, ANNEXES I, II, III**: the Parties agree that in the event that the details of the services are not yet specified in the Agreement (which may in particular be the case, if the Agreement is a frame(work) agreement), the information in the Annexes I to III (Attachment B) may need to be adjusted to fully and accurately reflect the circumstances surrounding the provision of services. The Parties shall mutually agree to the changes in writing

ATTACHMENT B

ANNEX I

A. LIST OF PARTIES

Data exporter(s)/Controller:

Name: Hillenbrand, Inc., acting on behalf of itself and its affiliates acting as the data exporter(s) and controller(s)

Address: 1 Batesville Blvd., Batesville, Indiana 47006 USA

Contact person's name, position and contact details: Valerie M. Talkers Senior Counsel – Employment Global Privacy Lead

Tel.: 1+**(812)-931-5381**; e-mail: **valerie.talkers@hillenbrand.com.**

By: ____

Name: ______________________________________

Title: _______________________________________

Date: ______________________________

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

Name: Defmacro Software Private Limited

Address: _______________________________________

Contact person's name, position and contact details: Ayush Gupta, Global DPO, DPO@cleartax.com

By: ____

Name: ______________________________________

Title: _______________________________________

Date: ______________________________

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

...

Categories of personal data transferred

...

Sensitive data transferred

...

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

EU:

Link to all EU competent supervisory authorities:

https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-de

Switzerland:
Federal Data Protection and Information Commissioner

(Eidgenoessischer Datenschutz- und Oeffentlichkeitsbeauftragter)

Feldeggweg 1

CH – 3003 Bern

Telephone: 0041 (0)58 462 43 95

Fax: +41 (0)58 465 99 96

United Kingdom:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow
Cheshire
SK9 5AF
England
Telephone: 0044 (0) 303 123 1113
Fax: 01625 524510

ANNEX II

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Annex II describes the technical and organizational security measures implemented by the Vendor (aka data importer) (including any relevant certifications) in accordance with the Agreement, the DPA, and applicable Data Protection Laws 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.

1. DATA SECURITY GOVERNANCE

Vendor maintains internal organizational and governance procedures to appropriately manage information throughout its lifecycle. Vendor regularly tests, assesses, and evaluates the effectiveness of its data security standards and controls.

- Vendor runs a robust Cybersecurity Awareness Program; and
- Vendor maintains a process for conducting personal information protection impact assessments; and
- Vendor runs a Risk Management Framework including external Pen Testing.
- Vendor conducts training of staff with access to personal data on regular basis, including training on the requirements of applicable data protection law, the risks and danger in connection with personal data processing and the security requirements implemented.
- Vendor has appointed one or more security officers in charge of coordinating and controlling the security measures.
- Vendor conducts continuing review of its security programs and procedures are to ensure that they are in compliance with applicable laws.
- Logging, tracking, and investigation of information security incidents, including personal data breaches.

2. PHYSICAL ACCESS CONTROL

Vendor uses a variety of measures appropriate to the function of the location to prevent unauthorized access to the physical premises where personal data is processed. Those measures include:

- Logging and alerting mechanisms;
- Surveillance systems including alarms and, as appropriate, CCTV monitoring;
- Receptionists and visitor policies;
- Access authorizations for employees and third parties are established and documented;
- Locking of server racks and secured equipment rooms within data centers; and
- Access to the data processing facilities where personal data is hosted is monitored, logged, and tracked.

3. VIRTUAL ACCESS CONTROL

Vendor implements appropriate measures to prevent its systems from being used by unauthorized persons. This is accomplished by:

- Individual, identifiable, and role-based user account assignment (following least privilege principles) and password protected access and authorization procedures;
- Centralized and standardized password management and password policies (minimum length/characters, change of passwords);
- User accounts are disabled after excessive failed log-on attempts;
- Automatic log-off in case of inactivity; and
- Anti-virus management; and
- MFA (Multi Factor Authentication); and
- Procedures in place to immediately remove access upon termination or departure.

4. **DATA ACCESS CONTROL**

Individuals that are granted use of Vendor systems are only able to access the data that are required to be accessed by them within the scope of their responsibilities and to the extent covered by their respective access permission (authorization) and such data cannot be read, copied, modified, or removed without specific authorization. This is accomplished by:

- Authentication at operating system level;
- Separate authentication at application level;
- Authentication against centrally-managed authentication system;
- Change control procedures that govern the handling of changes (application or OS) within the environment;
- Remote access has appropriate authorization and authentication;
- Logging of system and network activities to produce an audit-trail in the event of system misuse; and
- Implementation of appropriate protection measures for stored data and data in transit commensurate to risk, including encryption, pseudonymization, and password controls; and
- Controls in place to ensure data minimization, data quality, limited data retention, portability and erasure.

5. **DISCLOSURE CONTROL**

Vendor implements appropriate measures to prevent data from being read, copied, altered, or deleted by unauthorized persons during electronic transmission and during the transport of data storage media. Vendor also implements appropriate measures to verify to which entities' data are transferred. This is accomplished by:

- Data transfer protocols including encryption for data carrier/media;
- Profile set-up data transfer via secure file transfer methods (including printers);
- Encrypted VPN; and
- No physical transfers of backup media; and
- In the case that vendor is made aware of a data disclosure, immediate action is taken for remediation and notification.

6. **DATA ENTRY CONTROL**

Vendor implements appropriate measures to monitor whether data have been entered, changed, or removed (deleted), and by whom. This is accomplished by:

- Documentation of administration activities (user account setup, change management, access, and authorization procedures);
- Archiving of password-reset and access requests;
- System log-files enabled by default; and
- Storage of audit logs for audit trail analysis.

7. **INSTRUCTIONAL CONTROL**

Vendor implements appropriate measures to ensure that data may only be processed in accordance with the instructions of Hillenbrand. Those measures include:

- Binding policies and procedures on Vendor's employees; and
- Where Subprocessors are engaged in the processing of data, including appropriate contractual provisions to the agreements with Subprocessors to maintain instructional control rights.

8. **AVAILABILITY CONTROL**

Vendor maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:

- Extensive and comprehensive backup and recovery management systems;

- Documented disaster recovery and business continuity plans and systems;
- Storage and archive policies;
- Anti-virus, anti-spam, firewall, and IDS/IPS systems and management, including policies;
- Data centers are appropriately equipped according to risk, including physically separated back up data centers, uninterruptible power supplies (including backup generators), fail redundant hardware and network systems, and alarm and security systems (smoke, fire, water);
- Appropriate redundant technology on data storage systems; and
- All critical systems have backup and redundancy built into the environment; and
- Systems providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

9. SEPARATION CONTROL

Vendor implements appropriate measures to ensure that data that are intended for different purposes are processed separately. This is accomplished by:

- Access request and authorization processes provide logical data separation;
- Separation of functions (production /testing); and
- Segregation of duties and authorizations between users, administrators, and system developer.

10. ASSET MANAGEMENT CONTROL

Vendor maintains an adequate asset inventory of Hardware and Software Assets and ensures regular updates and patching as recommended and required by vendors and security standards in order to reduce the risk of unauthorized devices/software, disclosure, damage, or loss of data.

- Vendor ensures hardened OS images and removal of default credentials; and
- Have a tool to maintain up-to-date list of authorized software and hardware that are required in the organization; and
- Have in place a process from onboarding to retirement of an asset; and
- Vendor has a vulnerability management process and vulnerability management tools to continuously scan their environment; and
- Vendor has process in place for the secure disposal of assets.

ANNEX III

LIST OF SUBPROCESSORS

[Input by Vendor required]