DATA PROCESSING ADDENDUM

In connection with the supply and provision of products, software, solutions and services by Rockwell Automation to Customer pursuant to a separate agreement (the, "Agreement"), Rockwell Automation and its subcontractors may access, use, process, store or retain certain personal data of individuals associated with Customer (for example, employees and contractors of Customer and/or of its customers).

This Addendum applies to the extent Rockwell Automation (data processor) processes personal data, subject to Applicable Data Protection Laws, as a processor on behalf of Customer (data controller) under or in connection with the Agreement. To the extent Customer may be processing personal data on behalf of Rockwell Automation, subject to Applicable Data Protection Laws, the same provisions of this Addendum apply vice versa.

An overview of the categories of personal data, the categories of data subjects and the scope, nature, purpose, and duration of the processing of the personal data is provided in **Schedule 1**.

1. DEFINITIONS

1.1 Any terms not otherwise defined in the Agreement and in this Addendum shall have the meaning given to them in the Applicable Data Protection Laws, including, but not limited to "processor", "processing", "data controller", "personal data", "data subject".

1.2 "Applicable Data Protection Laws" mean, where applicable, the GDPR and/or other applicable laws and regulations in the relevant jurisdiction on the protection of the privacy and personal data of data subjects, as may be amended from time to time.

1.3 "Approved Subcontractor" a company or independent professional who is engaged and/or authorized by Rockwell Automation and will carry out activities and/or sub processing activities involving the processing of Customer Personal Data in connection with the Agreement, and approved pursuant to clauses 4.1 and/or 4.2.

1.4 "Customer Personal Data" means any personal data that Rockwell Automation and/or Approved Subcontractors may process as a processor on behalf of Customer under or in connection with the Agreement.

1.5 "GDPR" means 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, as may be amended or updated from time to time.

1.6 "Processing Instructions" are the documented instructions of Customer provided pursuant to Clause 2.1, provided these instructions are required, reasonable, technically feasible and within the scope of the Agreement.

1.7 "Personal Data Breach Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, and which requires notification to competent authorities and/or affected individuals, where applicable pursuant to Applicable Date Protection Laws.

2. PROCESSING UPON CUSTOMER'S INSTRUCTIONS

2.1 To the extent Rockwell Automation (data processor) processes Customer Personal Data, subject to Applicable Data Protection Laws, as a processor on behalf of Customer (data controller) under or in connection with the Agreement:

a. Rockwell Automation shall process the Customer Personal Data only in accordance with Customer's Processing Instructions as set out in this Addendum or otherwise in writing, unless required to do so otherwise by applicable law;

b. In addition, Customer hereby authorizes Rockwell Automation to take such actions involving the processing of Customer Personal Data on behalf of Customer as are reasonably necessary or useful for the performance of the Agreement, unless otherwise required by the Processing Instructions;

c. If applicable laws require Rockwell Automation to provide and/or otherwise process Customer Personal Data outside the scope of the Agreement, it shall notify Customer of any such requirement (unless applicable law prohibits such notification, for example on important grounds of public interest);

d. Rockwell Automation shall inform Customer if Rockwell Automation becomes aware of a Processing Instruction that, in Rockwell Automation's reasonable opinion, infringes Applicable Data Protection Laws, it being understood that this obligation does not constitute a general obligation of Rockwell Automation to monitor or interpret the laws applicable to Customer, and that such notification does not constitute legal advice to the Customer; and

e. Provided that, to the maximum extent permitted by applicable law, Rockwell Automation shall have no liability for any losses, costs, expenses, or liabilities arising from or in connection with any processing in accordance with the Processing Instructions.

2.2 Customer authorizes Rockwell Automation to provide instructions and authorizations that are similar to those provided in clause 2.1 to the Approved Subcontractors on behalf of the Customer.

2.3 Any additional instructions or changes to the Processing Instructions will be mutually discussed before their application.

3. COMPLIANCE WITH PRIVACY LAWS

3.1 Under and in connection with the Agreement, Customer and Rockwell Automation shall each, and shall cause their respective affiliated companies to, comply with Applicable Data Protection Laws.

3.2 Customer undertakes, warrants, and represents that:

a. Customer Personal Data is collected by Customer and provided to Rockwell Automation in accordance with Applicable Data Protection Laws;

b. Customer has the necessary lawful ground(s) and all necessary rights to provide, or allow access to, the Customer Personal Data to Rockwell Automation and Approved Subcontractors for processing in connection with the Agreement;

c. Customer will not do, nor omit to do, anything which may cause Rockwell Automation and Approved Subcontractors to be in breach of Applicable Data Protection Laws; and

d. The data subjects whose personal data are provided by or on behalf of Customer to, or are accessible by, Rockwell Automation and Approved Subcontractors have been informed of, and, if and to the extent required, have given valid consent to the processing of their personal data as envisaged in the Agreement.

4. SUBCONTRACTING

4.1 Rockwell Automation may subcontract to subcontractors any of its activities for its performance of the Agreement, requiring or involving processing of Customer Personal Data by these subcontractors, if:

a. Customer has provided its prior written approval; and

b. Rockwell Automation and each subcontractor have entered into a written agreement setting out data protection obligations that are similar to those set out in this Addendum.

4.2 Customer hereby gives its prior written approval for the subcontractors listed or described in **Schedule 3**, as well as the affiliated companies of Rockwell Automation.

4.3 If Rockwell Automation wishes to engage any new subcontractor, it will provide to Customer prior notice of its intention to engage such subcontractor.

4.4 If, within ten (10) business days from receipt of this notice, Customer does not object to Rockwell Automation's request, Customer will be deemed to have approved such subcontracting.

4.5 If, within ten (10) business days from receipt of the notice Customer objects on reasonable grounds relating to data protection (including data security) to Rockwell Automation's request, Rockwell Automation will use reasonable efforts to find a solution that is acceptable to Customer. If the parties have not been able to find a mutually acceptable solution within ten (10) business days from Rockwell Automation's receipt of Customer's notice of objection, Rockwell Automation will be entitled to terminate the works and services to be performed by Rockwell Automation under Agreement, for which it needs the proposed subcontractor or proposed alternative solutions.

4.6 Customer acknowledges and agrees that the procedure set out in sections 4.3 through 4.5 shall not apply if the need for Rockwell Automation to replace an Approved Subcontractor with a new subcontractor is urgent and necessary to perform under the Agreement. In such instance, Customer agrees that Rockwell Automation may immediately engage such subcontractor, provided that Rockwell Automation notifies Customer of such replacement as soon as reasonably practicable.

5. CROSS-BORDER TRANSFER OF PERSONAL DATA

Rockwell Automation may transfer Customer Personal Data into a country outside of the European Economic Area (in case of Customer Personal Data residing in the European Economic Area) and/or outside of the country of residence of the concerned individual(s) to the extent regulated by Applicable Data Protection Laws (such country outside of the European Economic Area and/or such other third country being referred to as a "Third Country") if:

5.1 In case of cross-border personal data transfer restrictions pursuant to the GDPR:

a. There has been an EU Commission finding of adequacy in respect of that Third Country;

b. The recipient has entered into a contract that contains model clauses that have been approved by the EU Commission or another competent public authority in accordance with Applicable Data Protection Laws (each such contract a "Data Transfer Agreement"); or

c. The cross-border transfer is covered by approved and maintained Binding Corporate Rules.

5.2 In case of other cross-border personal data transfer restrictions pursuant to other Applicable Data Protection Laws, the adequate level of protection system is applied as required by the relevant Applicable Data Protection Laws.

5.3 For the purpose of section 5.1.b, Customer (data controller) hereby grants to Rockwell Automation a power of attorney to conclude Data Transfer Agreements on behalf of the Customer, acting as controller, with any such recipients, which Rockwell Automation shall only exercise for the purpose of enabling the lawful transfer of Customer Personal Data to such recipients within the context of the Agreement. Upon Customer's request, Rockwell Automation shall provide copies of Data Transfer Agreements to the Customer. Alternatively, upon Rockwell Automation's request, Customer (data controller) agrees to enter into Data Transfer Agreements with recipients who are based or residing in a Third Country. In the event that there is a conflict between the Data Transfer Agreement and the Agreement, the Data Transfer Agreement prevails.

5.4 In case the specific statutory mechanism to authorize the applicable international data transfers is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid , the application of a suitable alternate mechanism that can lawfully support the transfer can be applied.

6. SECURITY AND CONFIDENTIALITY

6.1 Taking into account the scope and purposes of the processing, the types of personal data involved, the categories of affected data subjects, the possible privacy risks, the generally available state of the art and the costs of implementation, Customer and Rockwell Automation will implement and maintain reasonable technical and organizational security measures (as further specified in **Schedule 2**) to ensure a level of security, in respect of Customer Personal Data processed by Rockwell Automation under the Agreement, that is appropriate to the identified privacy risks, in particular to

protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Customer Personal Data.

6.2 Rockwell Automation ensures that persons who are authorised to process, or have access to, Customer Personal Data hereunder have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

6.3 Without prejudice to other applicable confidentiality obligations between the parties, Rockwell Automation will keep the Customer Personal Data confidential, use the Customer Personal Data for the purposes provided in this Addendum, and will not share it with third parties (other than Approved Subcontractors).

6.4 Customer acknowledges and agrees that, taking into account the nature, scope, risks and context of the processing of Customer Personal Data by Rockwell Automation within the context of the Agreement, Rockwell Automation's implementation of the technical and organizational security measures set forth in **Schedule 2** provide an appropriate level of security.

7. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

7.1 Rockwell Automation shall without undue delay upon termination or expiry of the Agreement, at Customer's written request, either delete or return to Customer all Customer Personal Data and copies thereof that are then under the control of Rockwell Automation, its affiliated companies, and its Approved Subcontractors.

7.2 This will not apply to the extent Rockwell Automation, any of its affiliated companies or Approved Subcontractors are required by law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems where the Customer Personal Data is securely isolated and protected from any further processing except to the extent required by law.

8. AUDITS AND DOCUMENTATION

Rockwell Automation will maintain records and information reasonably necessary to demonstrate compliance with its obligations under this Addendum. Rockwell Automation will allow, and collaborate with, Customer and/or or a third-party auditor appointed by the Customer, to audit Rockwell Automation's compliance with this Addendum, provided that:

8.1 The audit will, unless otherwise agreed with Rockwell Automation:

(a) Be subject to thirty (30) days' prior written notice from the Customer;

(b) Be conducted at reasonable intervals, but not more than once per calendar year;

(c) Be conducted during business hours and not unreasonably disrupt Rockwell Automation's business;

(d) Not interfere with the interests of Rockwell Automation's other customers;

(e) Not cause Rockwell Automation to breach its confidentiality obligations vis-à-vis its other customers, suppliers or any other organization;

(f) Not exceed a period of two (2) business days;

(g) Start with reviewing and assessing the information Rockwell Automation may provide through external, shared platforms it may support; and

(h) Relate only to the processing of Customer Personal Data by Rockwell Automation as a processor on behalf of Customer.

8.2 Customer shall, and shall cause its third-party auditor to, comply with Rockwell Automation's relevant security policies and appropriate confidentiality expectations.

8.3 When Rockwell Automation accepts that an audit goes beyond the parameters in this Addendum, Customer will reimburse Rockwell Automation for its reasonable costs and expenses associated with the audit.

8.4 Customer acknowledges that Rockwell Automation is regularly audited for compliance with various recognized standards. Rockwell Automation and the Approved Subcontractors are allowed to reject, or reduce the scope of, a requested audit, where they demonstrate their compliance with their obligations under or pursuant to this Addendum, by adhering to a code of conduct approved by the competent authority or regulator, by providing a generally recognized certification, or by providing an audit or information report issued by a generally accepted organization or independent third-party auditor.

9. ASSISTANCE

9.1 Customer is solely responsible for handling data subject requests relating to Customer Personal Data (for example, data subject access requests, data subject correction requests, etc.) and Customer will ensure that this is clearly reflected in the privacy notice that the Customer provides to its data subjects under Applicable Data Protection Laws.

9.2 If and to the extent possible and necessary for Customer to handle an audit by a competent authority, a complaint and/or a data subject request in accordance with Applicable Data Protection Laws, Rockwell Automation shall provide reasonable assistance to Customer.

9.3 In case a data subject files with Rockwell Automation a complaint and/or data subject request relating to Customer Personal Data, Rockwell Automation shall refer such request to Customer without undue delay, without being required to inform the data subject thereof.

9.4 If and to the extent possible, given the information that is available to Rockwell Automation, Rockwell Automation shall provide reasonable assistance to Customer in supporting Customer's compliance with its obligations under Applicable Data Protection laws with respect to (a) security of processing; (b) privacy risk reviews and data protection impact assessments; and (c) required communications with privacy supervisory authorities or regulators.

9.5 Reasonable costs and expenses incurred by or on behalf of Rockwell Automation in connection herewith shall be borne and reimbursed by Customer.

10. DATA BREACH NOTIFICATION

10.1 In case Rockwell Automation becomes aware of a (possible) Personal Data Breach Incident affecting Customer Personal Data it has access to or it otherwise processes and affecting the systems and/or activities that are under the control of Rockwell Automation, Rockwell Automation shall, without undue delay after it becomes aware of the incident:

(a) Notify Customer of the (possible) Personal Data Breach Incident;

(b) Investigate the (possible) Personal Data Breach Incident, take necessary actions to mitigate, remedy, and correct the incident, and keep the Customer informed of these actions.

(c) Use reasonable efforts to assist Customer, at Customer's request, in collecting and providing the information relating to the (possible) Personal Data Breach Incident which the Customer needs in order to assess the requirement of, and to comply with, the Customer's timely breach notification obligations to competent authorities and/or affected individuals pursuant to the Applicable Data Protection Laws (for example, a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; a description of the likely consequences of the incident; description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects).

10.2 In case Customer becomes aware of a (possible) Personal Data Breach Incident affecting the systems and/or activities that are under the control of Customer and also of Rockwell Automation or its Approved Subcontractors, Customer shall, without delay,

(a) Notify Rockwell Automation of the (possible) Personal Data Breach Incident; and

(b) Use reasonable efforts to assist Rockwell Automation, at Rockwell Automation's request, in collecting and providing the information relating to the (possible) Personal Data Breach Incident which Rockwell Automation needs in order to investigate the (possible) Personal Data Breach Incident, to take protective actions, and to comply with Rockwell Automation's obligations pursuant to the Applicable Data Protection Laws, if any.

10.3 Any damages, losses, costs and expenses incurred by or on behalf of Rockwell Automation in connection herewith, shall be borne and reimbursed by Customer, except if and to the extent the Personal Data Breach Incident occurred as a direct result of a breach of Rockwell Automation's obligations under this Addendum.

11. INDEMNIFICATION

11.1 Each party (indemnifying party) shall indemnify the other party (indemnified party) against any claims of data subjects, governmental authorities or other third parties, if

and to the extent this claim is a result of breach by the indemnifying party of its obligations under this Addendum and/or under Applicable Data Protection Laws. The limitation of liability and related provisions of the Agreements shall apply in addition.

11.2 In case a party receives such a third party claim, it will inform the other party thereof and will make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed).

12. DURATION

12.1 Rockwell Automation is authorized to process the Customer Personal Data hereunder until the expiration or termination of the Agreement, unless otherwise instructed by Customer, or until such data is returned or destroyed upon instruction from Customer.

13. MISCELLANEOUS

13.1 In case of inconsistency between the Agreement and this Addendum, this Addendum shall prevail. In case of inconsistency between this Addendum and the mandatory provisions of Applicable Data Protection Laws, the provisions of the Applicable Data Protection Laws shall prevail.

13.2 Subject to provisions of mandatory Applicable Data Protection Laws, the governing law applying to the Agreement shall apply for this Addendum.

SCHEDULE 1

Categories and Scope of Processing

THE NATURE AND THE PURPOSE OF THE PROCESSING

In connection with Rockwell Automation's performance under the Agreement, Rockwell Automation and Approved Subcontractors may gain access to, obtain copies of, or include in their deliverables certain Customer Personal Data provided by Customer.

In particular [PLEASE SPECIFY]

PERSONAL DATA CATEGORIES

[PLEASE CONFIRM] Non-sensitive Customer Personal Data, such as:

- Business contact details of data subjects, such as: name, title, phone number, email address, time zone, address data;
- System access, usage and authorization information and logs related to identified or identifiable data subjects;
- Industrial operational data and information technology data showing individual details of, and work performed by, data subjects;
- Customer acknowledges and agrees that no sensitive data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data, data concerning a person's sex life, or sexual orientation) is provided by the Customer as a part of Customer Personal Data.

CATEGORIES OF DATA SUBJECTS

Unless provided otherwise by Customer, employees, contractors, business partners, or other individuals associated with Customer or the customers of Customer.

SCHEDULE 2

Technical and Organizational Measures (TOMs)

Rockwell Automation implements, operates, and regularly maintains appropriate technical and organizational measures (TOMs) aligned to industry standards in order to protect the confidentiality, integrity, and availability of Customer Personal Data. The Customer acknowledges and agrees that the measures set forth herein and/or implemented are subject to technical progress and further development, allowing Rockwell Automation to unilaterally modify these measures provided that the functionality and security are not degraded. Without limiting the generality of the foregoing, Rockwell Automation will at a minimum maintain the technical and organizational measures as follows:

- **Information Security Governance.** Rockwell Automation will maintain an Information Security Management System (ISMS) including information security policies, standards, and guidelines following industry best practices and industry standard security frameworks. Rockwell Automation has effectively established an organization led by a senior leadership position responsible for deployment and communication of the ISMS (e.g. CISO). Rockwell Automation appointed one or more security officers responsible for coordinating and monitoring the rules and procedures related to information security.
- **Risk Management.** Rockwell Automation management performs an annual risk assessment in alignment with National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF). Management assesses the design and operating effectiveness of internal controls against the established controls framework. Results from risk assessment activities are reviewed to prioritize mitigation of any identified risks.
- **Employee Management.** Rockwell Automation ensures that it runs adequate pre-hire background checks on for its employees as permitted by applicable law. Employees are required to sign confidentiality, non-disclosure agreements and are contractually obligated to follow a code of ethical conduct.
- **Training and Awareness.** Rockwell Automation ensures that all its employees and contractors complete annual security awareness training which is regularly maintained to include any changes in policies, standards, and threat or attack vectors. Additional security awareness and training (e.g. newsletters, phishing exercises, etc.) are deployed monthly.
- **Access Control.** Rockwell Automation creates individual and unique identities for user and/or system accounts and prohibits the reuse, multi-purpose use, or sharing of identities. Identities no longer in use for any reason, including terminations, are subject to immediate disablement. Rockwell Automation ensures that only authorized personnel can access facilities, systems, and information based on job responsibilities and a need-to-know/least privilege principle. All access requests are processed by authorized role owners and regular access reviews are completed to ensure that the access assignments remain relevant and accurate. Rockwell Automation ensures that access to privileged systems and all remote access is additionally protected by using strong authentication methods (e.g. multi-factor) with extensive logging/monitoring of activities.
- **Physical and Environmental Security.** Rockwell Automation protects its facilities and information systems against unauthorized physical access, damage, and theft by using

appropriate perimeter, entry, monitoring, and environmental controls. Physical security controls deployed include, but are not limited to, entry/exit alarms, electronic badge and/or biometric access, and CCTV. Environmental controls deployed include, but are not limited to, temperature control, fire suppression, UPS, generators, and power/connectivity redundancy.

- **Operational Security.** Rockwell Automation protects its network and information systems assets by using appropriate security devices, software, and controls. Network security controls include, but are not limited to, hardened firewalls, routers, switches with content and packet filtering, IDS/IPS, segmentation, and event logging/monitoring. Information system asset controls include, but are not limited to, hardened operating systems, next-gen anti-virus/anti-malware, host-based firewall, and full disk encryption. Event logging from network and information system devices are collected within a restricted enterprise security and incident event manager (SIEM) and monitored by an authorized security operations center (SOC). Where Rockwell Automation personnel uses Rockwell Automation workstations/laptops, Rockwell Automation is responsible for applying standard technical and organizational security controls. Where Rockwell Automation personnel uses workstations from the Customer or accesses the customer network, system or infrastructure, Customer is responsible for applying Customers standard technical and organizational security controls.
- **Change Management.** Rockwell Automation ensures change management policies, standards, and procedures have been established, are maintained, and are enforced to track and manage changes made to its operational environment(s).
- **Configuration Management.** Rockwell Automation ensures security hardening and baseline configuration policies, standards, and procedures based on industry acceptable standards have been established, are maintained, and are enforced appropriately.
- **Incident Management.** Rockwell Automation ensures incident management and response policies, standards, and procedures have been established, are maintained, and are followed for any occurring incidents. Rockwell Automation will have identification, investigation, preservation, remediation, and communication procedures in place as deemed necessary and appropriate by the type of incident. Any incidents directly impacting or having the potential to impact Customer Personal Data will involve response actions detailed in section 10 of this Addendum.
- **Threat and Vulnerability Management.** Rockwell Automation ensures threat and vulnerability management policies, standards, and procedures have been established, are maintained, and are followed to continuously identify threats and remediate critical vulnerabilities. Appropriate vendor security updates and patches are applied to its information systems on a reoccurring monthly basis. Vulnerability scans are regularly performed to identify potential threats and/or risks in order to apply appropriate risk mitigation.
- **Disaster Recovery and Business Continuity.** Rockwell Automation maintains disaster recovery and business continuity policies, standards, and procedures to allow for the continuation and/or recovery of its critical business operations and services. Policies,

standards, and procedures are reviewed, tested, and updated as necessary on an annual basis.

- **System and Software Development.** Rockwell Automation follows a defined and secure software development lifecycle process. Authorized and role-trained employees are utilized to develop and maintain software. Secure coding, testing, and maintenance best practices include, but are not limited to, logged check in/check out of source code, version control, static/dynamic code analysis, code audits/reviews, vulnerability release management, and penetration testing when applicable. Rockwell Automation's development processes and procedures are in alignment with industry accepted practices (e.g. OWASP, IEC 62443).
- **Third Party Management.** Rockwell Automation ensures that its subcontractors and other third parties are assessed to be in compliance with its information security requirements and that any Approved Subcontractor is in compliance with the TOMs set forth in this document.

SCHEDULE 3

APPROVED SUBCONTRACTORS

Name of Subcontractor / Subcontractor Group	Purpose (e.g. Data Hosting, Software, Professional Services)	Link to applicable Data Privacy Terms of Subcontractor
PTC	Strategic partner of Rockwell Automation for the provision of OT/IT integration software and industrial digital transformation solutions	https://www.ptc.com/-/media/Files/PDFs/Legal-Policies/PTC----Standard-Data-Processor-TCs--v1-1-ENG.pdf?la=en&hash=05796A4D5E2F018479B03BF79A339980
Microsoft Azure	Cloud services provider	
Amazon Web Services	Cloud services provider	
Partner Network	Authorized Distributors, System Integrator Partners and other recognized partners of Rockwell Automation's Partner Network	https://www.rockwellautomation.com/en-us/company.html
Other	Services or work purchased by Rockwell Automation from third parties as an ancillary element for performing the Agreement, such as, telecommunication services, maintenance and use of service, cleaners, auditors or the disposal of data carriers	
Other	Affiliates of Rockwell Automation, supporting the implementation of the Agreement	