HONEYWELL'S DATA PROCESSING EXHIBIT FOR SUPPLIERS

The Honeywell Data Processing Exhibit for Suppliers ("**Data Processing Exhibit**") forms part of the Agreement between Honeywell and Supplier and applies to the extent Supplier processes Personal Data on behalf of Honeywell (or Honeywell's customer) in the course of providing the Services under the Agreement. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In event of conflict between this Data Processing Exhibit and the Agreement, this Data Processing Exhibit will control with respect to its subject matter.

1. Definitions

"**Agreement**" means the written or electronic agreement between Honeywell and Supplier for the provision of the Services to Honeywell.

"**Applicable Privacy Laws**" means applicable data protection, privacy, breach notification, or data security laws or regulations that may exist in any relevant jurisdiction such as, for example, the General Data Protection Regulation 2016/679 ("**GDPR**"), state and federal US privacy laws and the General Data Protection Law 13.709/2018.

"**Controller**" means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. The Controller may be Honeywell or Honeywell's customer.

"**Honeywell Personal Data**" means Personal Data Processed by Supplier on behalf of Honeywell in connection with Supplier's performance of its obligations under the Agreement.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure, or use of Honeywell Personal Data while Processed by Supplier and/or its Subprocessors under this Data Processing Exhibit.

"**Sell**" or "**sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data by one business to another business or a third party for monetary or non-monetary consideration. Sale does not include the sharing or transfer of Personal Data by Honeywell to Supplier for the provision of the Services on behalf of Honeywell under the Agreement.

"**Subprocessor**" means any Processor engaged by Supplier for the provision of the Services including Supplier's affiliates and service providers that process Honeywell Personal Data pursuant to the Agreement.

Regardless of Applicable Privacy Laws, the terms "**Data Subject,**" "**Personal Data,**" "**Processor,**" and "**Processing**" will have the meaning defined in the GDPR or analogous definitions in Applicable Privacy Laws.

2. Processing

2.1. Role of the Parties. As between Supplier and Honeywell, Supplier will Process Honeywell Personal Data under the Agreement as a Processor acting on behalf of Honeywell as the Controller (except where Honeywell acts as a Processor in which case Supplier is a Subprocessor).

2.2. Instructions. Supplier will Process Honeywell Personal Data in accordance with Honeywell's documented instructions unless required to so do by applicable law to which Supplier is subject. Supplier is not responsible for determining whether Honeywell's instructions are compliant with applicable law. However, if Supplier is of the opinion that Honeywell's instruction infringes Applicable Privacy Laws, it will inform Honeywell of that legal requirement unless applicable law prohibits such notification. Any additional or alternate instructions must be agreed between the Parties in writing, including the costs (if any) associated with complying with such instructions. Upon notice in writing, Honeywell may terminate the Agreement if Supplier does not comply with

Honeywell's lawful instructions that are within the scope of the Agreement to the extent such instructions are necessary to enable Honeywell to comply with Applicable Privacy Laws. Supplier will refund to Honeywell any unused prepaid fees or waive any termination fees or minimum commitment if Honeywell terminates the Agreement on these grounds.

2.3. Purpose limitation. Supplier will only process Honeywell Personal Data as permitted under the Agreement and Applicable Privacy Laws. Supplier is prohibited from selling, retaining, using or disclosing any Honeywell Personal Data to any third party for the commercial benefit of Supplier or any third party, or to otherwise Process the Honeywell Personal Data outside of the direct business relationship between the Parties. Supplier certifies that it understands and will comply with all restrictions placed on its Processing of the Honeywell Personal Data.

2.4. Processing Details. The subject matter, duration of Processing, nature and purpose of Processing, the type of Honeywell Personal Data and categories of Data Subjects are specified in Annex 1 to this Data Processing Exhibit.

3. Subprocessors

3.1. Authorisation to use Subprocessors. Honeywell authorizes Supplier to use Subprocessors to Process Honeywell Personal Data provided Supplier contractually requires Subprocessors to abide by terms no less restrictive than this Data Processing Exhibit. Supplier will be liable to Honeywell for the performance of its Subprocessor's data protection obligations under the Agreement.

3.2. Notification of intended changes. Supplier will notify Honeywell of any intended changes to its Subprocessors and will give Honeywell thirty (30) days to object after receipt of the notification. If Honeywell legitimately objects to a Subprocessor on reasonable data protection grounds and the Parties do not resolve the matter within one month following notification of the same to Honeywell, Honeywell may suspend or terminate the Agreement without penalty on written notice.

4. Security

4.1. Security Measures by Supplier. To ensure the security of Honeywell's Personal Data, Supplier will implement the technical and organizational measures specified in the ***Honeywell Security Terms and Conditions for Suppliers Exhibit*** attached to the Agreement and incorporated herein by reference. Supplier's security controls will comply with Applicable Privacy Laws and take into account industry standards, the nature of the Honeywell Personal Data, and the risks represented by Supplier's Processing of the Honeywell Personal Data by virtue of the physical, logical, or natural environment in which the Honeywell Personal Data is stored or Processed. Supplier will apply specific restrictions and additional safeguards if it Processes sensitive personal data (as defined under Applicable Privacy Laws) on behalf of Honeywell.

4.2. Confidentiality. Supplier will ensure that only authorised personnel who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality may Process Honeywell Personal Data for the purposes of performing the Services under the Agreement.

5. **Security Incident**

5.1. Notification. Supplier will notify Honeywell without undue delay after becoming aware of a Security Incident in relation to the Services under the Agreement. Supplier will investigate the Security Incident and provide Honeywell with relevant information as required under Applicable Privacy Laws. Such information must at least include a description of the Security Incident including where possible, the nature of the Honeywell Personal Data concerned, the categories and approximated number of the Data Subjects and Personal Data records concerned, the likely consequences of

the Security Incident and the measures taken or proposed by Supplier to remediate the Security Incident and mitigate its effects.

5.2. Assistance. Supplier will cooperate with Honeywell in notifying the Security Incident to a supervisory authority, customer of Honeywell, and/or affected Data Subjects and to carry out any recovery or other action necessary to remedy the Security Incident as required under Applicable Privacy Laws. At Honeywell's option, Supplier will either: (a) provide, at Supplier's own cost and expense and pursuant to Honeywell's direction, notice to the Data Subjects affected by the Security Incident in a manner that is consistent with Applicable Privacy Laws and, to the extent deemed appropriate by Honeywell under the circumstances, at least one (1) year of credit-monitoring and identity theft insurance services; or (b) reimburse Honeywell for all costs incurred to provide the same. Supplier will respond promptly and fully cooperate to all inquiries from Honeywell, any supervisory authority or government authority regarding the Security Incident. Upon request and periodically as additional information becomes available, Supplier will, without undue delay, provide Honeywell with updates on the status of the Security Incident until the matter has been fully addressed and remediated.

5.3. Third party communications. Prior to Supplier's release, publication, transmission, or communication to any third party (including any supervisory authority, the media, or any affected Data Subject) relating to a Security Incident (collectively, "**Breach Communications**"), Supplier must first obtain prior written approval from Honeywell to the extent that (a) Honeywell or any of its Affiliates are specifically named or referenced in such Breach Communications; (b) Honeywell Personal Data or Honeywell systems are affected by the Security Incident; (c) the Breach Communications are directed at Honeywell's or its Affiliates' employees, suppliers, or customers; or (d) Honeywell may have certain independent legal, regulatory, or contractual obligations as a result of the Security Incident.

6. **Demonstrating Compliance.** Upon Honeywell's written request and subject to obligations of confidentiality, Supplier will (and shall ensure that its Subprocessors will) provide to Honeywell all information necessary to demonstrate its compliance with this Data Processing Exhibit. Honeywell (or an independent auditor mandated by Honeywell) may audit Supplier's compliance with such obligations at regular intervals or if there are indications of non-compliance with the terms of this Data Processing Exhibit ("**Audits**"). At Honeywell's request, upon reasonable notice, Supplier will also permit and contribute to onsite audits or inspections. In deciding on a review or Audit, Honeywell may consider any relevant certifications (such as SOC 2 Type II report) held by Supplier. Supplier will deal promptly and adequately with Audit inquiries from Honeywell. If Supplier, or any Subprocessor, is in breach of any of its obligations under the Agreement relating to Honeywell Personal Data, Honeywell may (without prejudice to any other rights or remedies it may have) suspend the transfer of Honeywell Personal Data to Supplier until the breach is remedied.

7. Data Transfers

7.1. Authorisation for Data Transfers. Honeywell hereby authorizes Supplier and its Subprocessors to transfer Honeywell Personal Data to locations outside of its country of origin for the performance of the Agreement provided that Supplier ensures such data transfers comply with Applicable Privacy Laws.

7.2. Data Export Restrictions. If Honeywell transfers Honeywell Personal Data from the European Economic Area, UK, Switzerland or from any other jurisdiction that restricts the cross-border transfer of Honeywell Personal Data to locations outside that jurisdiction, Honeywell will be bound by the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 including the provisions in Modules 2 and 3, as applicable, and the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses made

under s119A(i) of the UK's Data Protection Act 2018 ("**Processor SCCs**") in the capacity of "data exporter," and Supplier in the capacity of "data importer" as those terms are defined therein. The Processor SCCs will be deemed to have been signed by each Party and are hereby incorporated by reference into the Agreement in their entirety as if set out in full as an annex to this Exhibit. The Parties acknowledge that the information required to be provided in the appendices to the Processor SCCs is set out in Annex 1 below as a "description of the transfer" and "*Honeywell's Security Terms and Conditions for Suppliers Exhibit*" set out in the Agreement as a "description of the technical organisational measures." If there is a conflict between the provisions of this Data Processing Exhibit or the Agreement and the Processor SCCs, the Processor SCCs will prevail.

8. **Cooperation**. Supplier will promptly notify Honeywell of any request or complaint that it receives from a Data Subject, supervisory authority or any third party relating to the Processing of Honeywell Personal Data under the Agreement. Supplier will not respond to any request or complaint itself unless authorised to do so by Honeywell or as required by applicable law. Supplier will cooperate with Honeywell in fulfilling its obligations to respond to Data Subjects, conduct a privacy impact assessment or prior consultation with the supervisory authorities, provided that Honeywell reimburses Supplier for all reasonably incurred costs. If Supplier receives a Data Subject request relating to Honeywell Personal Data, Supplier will refer such Data Subject request to Honeywell within two (2) business days following receipt of the request.

9. **Termination**. Upon termination of the Agreement, Supplier will return, delete or anonymize all Honeywell Personal Data in accordance with the Agreement except to the extent Supplier is required by applicable law to retain Honeywell Personal Data in which case the terms of this Data Processing Exhibit will continue to apply to the retained Honeywell Personal Data.

10. **Survival**. The undertakings in this Data Processing Exhibit shall remain in force even after termination or expiration of the Agreement and/or the applicable Statements of Work for whatever reason.

11. **Notices.** Notwithstanding anything to the contrary in the Agreement, all notices that Supplier is required to provide to Honeywell pursuant to this Data Processing Exhibit must sent by email with a read receipt to HoneywellPrivacy@Honeywell.com

12. **Affiliates.** This Data Processing Exhibit is entered into by Honeywell for and on behalf of itself and each of its Affiliates described in Annex 2 to this Data Processing Exhibit.

ANNEX 1 TO HONEYWELL'S DATA PROCESSING OBLIGATIONS FOR SUPPLIERS EXHIBIT

DESCRIPTION OF THE PROCESSING AND TRANSFER CONTROLLER TO PROCESSOR

A. LIST OF THE PARTIES	
Controller/Data Exporter:	Name: Honeywell International Inc., its affiliates, and subsidiaries Address: 855 S. Mint St., Charlotte, NC 28202, USA Contact: Chief Privacy Officer Email: HoneywellPrivacy@honeywell.com
Processor/Data Importer	The full name, address and contact details for the Party is set out in the Agreement.
B. DETAILS OF PROCESSING/TRANSFER	
CATEGORIES OF DATA SUBJECTS	Dependent on the Data Exporter's use of the Data Importer's Services, the Data Exporter may elect to include Personal Data from any of the following types of data subjects: • Employees, contractors, temporary workers, directors, company officers, shareholders and agents (current, former, prospective) of data exporter • Beneficiaries, dependents, and relatives of the data subject • Channel Partners, distributors, sales partners, and business partners • Advisors, trainers, consultants, service providers and other third parties • Users (e.g., customers) and end users of data exporter's Product and Services • Any other data subject as described in the Agreement.
CATEGORIES OF PERSONAL DATA	Dependent on the Data Exporter's use of the Data Importer's Services, the Data Exporter may elect to include Personal Data from any of the following categories of Personal Data: • Basic personal data (for example first name, last name, initials, email address, job title, country of residence, mobile phone number) • HR and recruitment data (for example basic employment data, education data, demographic data, employment status, job and position data, worked hours, holidays, assessments, performance appraisals, salary, benefits, work permit details, availability, terms of employment, tax details, payment details, insurance details, travel information and recruitment information such as curriculum vitae, employment history, education history details) • Authentication data (for example username, password, security question, audit trail) • Unique identification numbers and signatures (for example IP addresses, unique identifiers in tracking cookies or similar technology) • Citizenship and residency information (for example nationality, citizenship, naturalization status, immigration status, passport data, details of residency or work permit) • Biometric Information (for example facial recognition, fingerprints, and iris scans) • Commercial Information (for example history of purchases, special offers and payment history) • Support Services (for example personal data collected through the provision of support services online or interactive communications) • IT systems and operational information (for example unique identifiers, voice, video and data recordings, tracking of information regarding the patterns of hardware, software, device and internet usage, IP addresses, domains, apps installed, browsing and support logs, incidental access of the content of email communications and data relating to the sending, routing and delivery of emails whilst providing support services) • Location data (for example, mobile device ID, geo-location network data, location data derived from use of wi-fi access points) • Device identification (for example UUID, IMEI-number, SIM card number, MAC address); • Training and development (for example trainee data, training history, individual development plans, trainer information and training schedules) • Photos, video and audio (for example webcam or voice recordings)

SPECIAL CATEGORIES OF DATA (IF APPLICABLE)	Dependent on the Data Exporter's use of the Data Importer's Services, the Data Exporter may elect to include Personal Data from any of the following special categories of Personal Data which is in the scope of the Services: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, gender orientation, data relating to criminal convictions or offences or precise geolocation data or any other type of personal data provided under the Agreement that is considered sensitive under Applicable Privacy Laws.
FREQUENCY OF THE TRANSFER	The data transfers under the Agreement will take place on a continuous basis.
NATURE OF THE PROCESSING	Data Importer and its subprocessors are providing Services or fulfilling contractual obligations to the Data Exporter as described in the Agreement. These Services may include the processing of Personal Data by Data Importer and/or its subprocessors.
PURPOSE OF PROCESSING/TRANSFER	Dependent on the Data Exporter's use of the Data Importer's Services, the Data Exporter's Personal Data is processed, and transfer is made for the following purposes: • Relationship management: facilitating communication with customers, employees and users for the services performed under the Agreement. • HR and recruitment: the processing of applicant and employee personal data for the purposes of administering, organizing, and managing the applicant and employment relationship. • Service management: the provision and deployment of products and related services, consultancy, data migration, installation of systems and software, provision of support and maintenance services, training, channel and/or supplier administration and support. • Channel: administration and management of channel partners, distributors and/or sales partners. • Marketing: administration and management of marketing databases for direct marketing purposes, conduct of marketing activities/campaigns. • Management of electronic identity and communication: identity management, security management, confidentiality of data exporter and data exporter's customers and employees. • Operating and managing the IT and communications systems, managing product and service development, improving existing and developing new products and services, research and development, managing company assets, allocating company assets and resources, strategic planning, project management, business continuity. • Training: administration of learning managements systems, facilitation of onsite and online learning. • Research in any field including scientific and technical research. • Any other scope and purpose as described in the Agreement.
RETENTION	The Data Exporter's Personal Data will be retained in accordance with the Agreement unless applicable law requires storage of the Personal Data for a longer period.
COMBINATION OF DATA	Personal Data received from the Data Exporter is combined with Personal Data collected by the Data Importer unless otherwise prohibited by the Agreement.

TRANSFER TO SUBPROCESSORS	The Data Importer may process and transfer Personal Data to subprocessors in relation to the performance of the Agreement and in accordance with the following scope:
	• **Subject Matter**
	  ○ The subject matter of the processing under the Agreement is the Personal Data.
	• **Nature of the processing**
	  ○ Data importer and its subprocessors are providing Services or fulfilling contractual obligations to the data exporter as described in the Agreement. These Services may include the processing of Personal Data by data importer and/or its subprocessors.

	• **Duration** ○ The duration of the processing under the Agreement is determined by the data exporter and as set forth in the Agreement.
LIST OF SUBPROCESSORS	The list of sub-processors is available upon request.
C. COMPETENT SUPERVISORY AUTHORITY	
The competent supervisory authority shall be the supervisory authority which has jurisdiction in relation to the activities of the Data Exporter as controller under applicable privacy laws or, where it is not established in applicable jurisdiction, where its representative has been established pursuant to applicable legal requirements or, if the Data Exporter does not have to appoint a representative, where the data subjects whose Personal Data are transferred are located.	
D. GOVERNING LAW AND CHOICE OF FORUM	
GOVERNING LAW	For the purposes of Clause 17 of the SCCs, the Parties select the law of Ireland.
CHOICE OF FORUM	For the purposes of Clause 18 of the SCCs, the Parties select the courts of Ireland.
E. OTHER	
Where the SCCs identify optional provisions (or provisions with multiple options) the following will apply:	For Clause 7 (Docking Clause), the optional provision will apply
	For Clause 9 (a), option 2 will apply. The parties will follow the process agreed in Section 3 (Subprocessing) of the Honeywell Data Processing Exhibit.
	For Clause 11(a) (Redress) – the optional provision will not apply

ANNEX 2 TO HONEYWELL'S DATA PROCESSING OBLIGATIONS FOR SUPPLIERS EXHIBIT

This Data Processing Exhibit is entered into by Honeywell for and on behalf of itself and its Affiliates identified on the list available at https://www.honeywell.com/us/en/honeywell-affiliates as updated from time to time.