Interworks Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the InterWorks General Services Terms and Conditions, as updated from time to time, or other agreement between Customer and InterWorks governing Customer's use of InterWorks services (the "**Terms**"). This DPA is an agreement between you and the entity you represent ("**Customer**") and **InterWorks**, as defined in the Terms. Unless otherwise defined in this DPA or in the Terms, all capitalized terms used in this DPA will have the meanings given to them in Section 15 of this DPA.

1. Data Processing.
   - 1.1. Scope and Roles. This DPA applies when Customer Data is processed by InterWorks. In this context, InterWorks will act as processor to Customer, who can act either as controller or processor of Customer Data.
   - 1.2. Details of Data Processing.
     - 1.2.1. Subject matter. The subject matter of the data processing under this DPA is Customer Data.
     - 1.2.2. Duration. As between InterWorks and Customer, the duration of the data processing under this DPA is determined by Customer.
     - 1.2.3. Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.
     - 1.2.4. Nature of the processing. Communication and management of Services as described in an Ordering Document entered into by Customer from time to time.
     - 1.2.5. Type of Customer Data. Customer Data provided to InterWorks pursuant to the provision of Services by InterWorks.
     - 1.2.6. Categories of data subjects. The data subjects could include Customer's employees, suppliers, and customers.
   - 1.3. Compliance with Laws. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. Customer Instructions. The parties agree that this DPA and the Terms (including the applicable Ordering Document and any instructions communicated to InterWorks during provision of the Services) constitute Customer's documented instructions regarding InterWorks' processing of Customer Data ("**Documented Instructions**"). InterWorks will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between InterWorks and Customer, including agreement on any additional fees payable by Customer to InterWorks for carrying out such instructions. Customer is entitled to terminate this DPA and the Terms if InterWorks declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Given the nature of the processing, Customer agrees that it is unlikely InterWorks can form an opinion on whether Documented Instructions infringe the GDPR. If InterWorks forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. Confidentiality of Customer Data. InterWorks will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends InterWorks a demand for Customer Data, InterWorks will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, InterWorks may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then InterWorks will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless InterWorks is legally prohibited from doing so.

4. Confidentiality Obligations of InterWorks Personnel. InterWorks restricts its personnel from processing Customer Data without authorization by InterWorks as described in the InterWorks Security Measures (Annex 1). InterWorks imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection, and data security.

5. Security of Data Processing.
   - 5.1. InterWorks has implemented and will maintain the technical and organizational measures for InterWorks Systems as described in the InterWorks Security Measures and this Section. In particular, InterWorks has implemented and will maintain the following technical and organizational measures:
     - 5.1.1. security of the InterWorks Systems as set out in Section 1.1 of the InterWorks Security Measures;
     - 5.1.2. physical security of the facilities as set out in Section 1.2 of the InterWorks Security Measures;

5.1.3. measures to control access rights for InterWorks employees and contractors to the InterWorks Systems as set out in Section 1.1 of the InterWorks Security Measures; and

5.1.4. processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by InterWorks as described in Section 2 of the InterWorks Security Measures.

5.2. Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from InterWorks or directly from a third party supplier:

5.2.1. pseudonymization and encryption to ensure an appropriate level of security;

5.2.2. measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services that are operated by Customer;

5.2.3. measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

5.2.4. processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

6.1. Authorized Sub-processors. Customer provides general authorization to InterWorks' use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. A list of current Sub-processors, which shall be updated when new sub-processors are engaged, can be accessed at: www.interworks.com/dpt/subprocessors, and InterWorks will provide Customer with a mechanism to obtain notification of such updates. InterWorks may also directly notify Customer in the event additional Sub-processors may be required to process Customer Data in connection with the Services. If Customer does not approve of any new Sub-processor, such approval not to be unreasonably withheld, Customer shall notify InterWorks of such determination and the parties agree to work together in good faith to resolve such concerns. To the extent that they cannot be resolved, InterWorks shall either cease its use of the Sub-processor to process the Customer Data or notify Customer that it may terminate that portion of the Services that require the use of the Sub-processor in accordance with the.

6.2. Sub-processor Obligations. Where InterWorks authorizes a Sub-processor as described in Section 6.1:

6.2.1. InterWorks will restrict the Sub-processor's access to Customer Data to only what is necessary for the provision of Services, and InterWorks will prohibit the Sub-processor from accessing Customer Data for any other purpose;

6.2.2. InterWorks will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by InterWorks under this DPA, InterWorks will impose on the Sub-processor the same contractual obligations that InterWorks has under this DPA; and

6.2.3. InterWorks will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause InterWorks to breach any of InterWorks' obligations under this DPA.

7. InterWorks Assistance with Data Subject Requests. If a data subject makes a request to InterWorks, InterWorks will promptly forward such request to Customer once InterWorks has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes, on its behalf, and on behalf of its controllers when Customer is acting as a processor, InterWorks to respond to any data subject who makes a request to InterWorks, to confirm that InterWorks has forwarded the request to Customer. The parties agree that InterWorks forwarding data subjects' requests to Customer in accordance with this Section represent the scope and extent of InterWorks' required assistance.

8. Security Incident Notification.

8.1. Security Incident. InterWorks will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

8.2. InterWorks Assistance. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), InterWorks will cooperate with and assist Customer by including in the notification under Section 8.1(a) such information about the Security Incident as InterWorks is able to disclose to Customer, given the nature of the processing, the information available to InterWorks, and any restrictions on disclosing the information, such as confidentiality. Given the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

8.3. Unsuccessful Security Incidents. Customer agrees that an unsuccessful Security Incident will not be subject to this Section 8. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of InterWorks' equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents.

8.4. Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means InterWorks selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information with InterWorks. Customer agrees that InterWorks' obligation to report or respond to a Security Incident under this Section 8 is not and will not be construed as an acknowledgement by InterWorks of any fault or liability of InterWorks with respect to the Security Incident.

9. Testing and Audits.

9.1. InterWorks Testing. InterWorks uses internal processes and testing to verify the adequacy of its security measures. This testing: (a) will be performed at least annually; (b) will be performed using to ISO 27002 standards or such other alternative standards that are substantially equivalent to ISO 27002; and (c) will be performed by at InterWorks' selection and expense.

9.2. Testing Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, InterWorks' internal staff will communicate appropriately with Customer to reasonably verify InterWorks' compliance with its obligations under this DPA.

9.3. Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the processing and the information available to InterWorks, InterWorks will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information InterWorks makes available under this Section 9.

9.4. Customer Audits. If Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR or the Standard Contractual Clauses, Customer may issue such request by sending InterWorks written notice as provided for in the Terms. If InterWorks declines to provide any such requested audits, including inspections, Customer is entitled to terminate the Services in accordance with the Terms.

10. Transfers of Personal Data.

10.1. Regions. Customer may request the location(s) where Customer Data will be processed within the InterWorks Systems (each a "Region"), including Regions in the EEA. If such request is accepted by InterWorks in writing, InterWorks will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

10.2. Application of Standard Contractual Clauses. The Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "Data Transfer").

10.2.1. When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

10.2.2. When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Given the nature of the processing, Customer agrees that it is unlikely that InterWorks will know the identity of Customer's controllers because InterWorks has no direct relationship with Customer's controllers and therefore, Customer will fulfill InterWorks' obligations to Customer's controllers under the Processor-to-Processor Clauses.

10.2.3. Alternative Transfer Mechanism. The Standard Contractual Clauses will not apply to a Data Transfer if InterWorks has adopted binding corporate rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

11. Termination of the DPA. This DPA will continue in force until the termination of the Services subject to the Terms (the "Termination Date").

12. Return or Deletion of Customer Data. Processing by InterWorks shall only take place for the duration of the Services. After the end of the Services, InterWorks shall, at Customer's choice, delete all Customer Data and certify to Customer that it has done so, or return to Customer all Customer Data and delete existing copies. Until Customer Data is deleted or returned, InterWorks shall continue to ensure compliance with this DPA. In case of local laws applicable to InterWorks that prohibit return or deletion of the Customer Data, InterWorks warrants

that it will continue to ensure compliance with this DPA and will only process it to the extent and for as long as required under that local law.

13. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by InterWorks, InterWorks will inform Customer without undue delay. InterWorks will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.
14. Entire Agreement; Conflict. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Terms will remain in full force and effect. If there is a conflict between the Terms and this DPA, the terms of this DPA will control, except that an Ordering Document will control over this DPA if such superseding language is specifically described in the terms of the Ordering Document. Nothing in this document varies or modifies the Standard Contractual Clauses.
15. Definitions. Unless otherwise defined in the Terms, all capitalized terms used in this DPA will have the meanings given to them below:
    - 15.1. "InterWorks Systems" means InterWorks' servers, networking equipment, and host software systems (for example, virtual firewalls) that are within InterWorks' control and are used to provide the Services.
    - 15.2. "InterWorks Security Measures" means the security standards attached to this DPA as Annex 1.
    - 15.3. "controller" has the meaning given to it in the GDPR.
    - 15.4. "Controller-to-Processor Clauses" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
    - 15.5. "Customer Data" means any "personal data" (as defined in the GDPR) that is provided to InterWorks in connection with the Services.
    - 15.6. "EEA" means the European Economic Area.
    - 15.7. "GDPR" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
    - 15.8. "processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.
    - 15.9. "processor" has the meaning given to it in the GDPR.
    - 15.10. "Processor-to-Processor Clauses" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
    - 15.11. "Security Incident" means a breach of InterWorks' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.
    - 15.12. "Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 10.2.1 and 10.2.2.
    - 15.13. "Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1
InterWorks Security Measures
Capitalized terms not otherwise defined in this document have the meanings assigned to them in the DPA.

1. Information Security Program. InterWorks will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the InterWorks Systems, and (c) minimize security risks, including through risk assessment and regular testing. InterWorks will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:
    1.1. Network Security. The InterWorks Systems will be electronically accessible to employees, contractors, and any other person as necessary to provide the Services. InterWorks will maintain access controls and policies to manage what access is allowed to the InterWorks Systems from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. InterWorks will maintain corrective action and incident response plans to respond to potential security threats.
    1.2. Physical Security.
        1.2.1. Physical Access Controls. Physical components of the InterWorks Systems are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
        1.2.2. Limited Employee and Contractor Access. InterWorks provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to them, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of InterWorks or its affiliates.
        1.2.3. Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. InterWorks also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and may be audited.
2. Continued Evaluation. InterWorks will conduct periodic reviews of the security of its InterWorks Systems and adequacy of its information security program as measured against industry security standards and its policies and procedures. InterWorks will continually evaluate the security of its InterWorks Systems to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.