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 connection with the Services. This DPA addresses the requirements of:

(a) The EU General Data Protection Regulation (Regulation 2016/679) ("EU GDPR");

(b) The UK General Data Protection Regulation as incorporated into UK law by the Data Protection Act 2018 ("UK GDPR");

(c) The Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles ("Australian Privacy Law");

(d) The Singapore Personal Data Protection Act 2012 ("Singapore PDPA");

(e) Applicable U.S. state privacy laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and other substantially similar state privacy laws ("U.S. State Privacy Laws"); and

(f) The Canadian Personal Information Protection and Electronic Documents Act and substantially similar provincial laws, including Quebec's Act Respecting the Protection of Personal Information in the Private Sector ("Canadian Privacy Laws").

The provisions of this DPA shall apply to the extent the applicable Data Protection Law governs the processing of Customer Data. Where a jurisdiction-specific schedule is attached to this DPA, the terms of that schedule shall supplement (and, in the event of conflict, supersede) the general terms of this DPA with respect to Customer Data subject to that jurisdiction's laws. In the context of EU GDPR and UK GDPR, InterWorks will act as processor to Customer, who can act either as controller or processor of Customer Data. In the context of other Data Protection Laws, InterWorks will act in the analogous role (e.g., "service provider" under CCPA/CPRA, "data intermediary" under Singapore PDPA).

1.2. Details of Data Processing.

(a) Subject matter. The subject matter of the data processing under this DPA is Customer Data.

(b) Duration. As between InterWorks and Customer, the duration of the data processing under this DPA is determined by Customer.

(c) Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

(d) Nature of the processing. Communication and management of Services as described in an Ordering Document entered into by Customer from time to time.

(e) Type of Customer Data. Customer Data provided to InterWorks pursuant to the provision of Services by InterWorks.

(f) 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.

1.4 Applicable Schedules. The jurisdiction-Specific Schedules attached to this DPA shall apply as follows:

If Customer Data is subject to:	*This schedule applies:*
UK GDPR	Schedule 1 (UK)
Australian Privacy Law	Schedule 2 (Australia)
Singapore PDPA	Schedule 3 (Singapore)
U.S. State Privacy Laws	Schedule 4 (U.S.)
Canadian Privacy Laws	Schedule 5 (Canada)

Multiple Schedules may apply simultaneously if Customer Data is subject to multiple Data Protection Laws. In the event of conflict between Schedules, the Schedule providing greater protection to data subjects shall prevail.

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:

(a) security of the InterWorks Systems as set out in Section 1.1 of the InterWorks Security Measures;
(b) physical security of the facilities as set out in Section 1.2 of the InterWorks Security Measures;
(c) 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
(d) 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:

(a) pseudonymization and encryption to ensure an appropriate level of security;
(b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services that are operated by Customer;
(c) 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
(d) 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 will be provided upon request, and InterWorks will provide Customer with a mechanism to obtain notification of 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 Terms.

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

(a) 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;

(b) 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

(c) 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, and in any event within forty-eight (48) hours, after becoming aware of the Security Incident; (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident; and (c) provide Customer with the following information to the extent known: (i) a description of the nature of the Security Incident, including the categories and approximate number of individuals and records concerned; (ii) the likely consequences of the Security Incident; (iii) the measures taken or proposed to address the Security Incident; and (iv) the name and contact details of InterWorks' point of contact for further information.

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, United Kingdom, or other jurisdictions. 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. EU Data Transfers. The Standard Contractual Clauses approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 will apply to Customer Data that is transferred from the EEA to any country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (a "Third Country").

(a) When Customer is acting as a controller, the Controller-to-Processor Clauses (Module Two) will apply.

(b) When Customer is acting as a processor, the Processor-to-Processor Clauses (Module Three) will apply.

10.3. UK Data Transfers. For transfers of Customer Data from the United Kingdom to a Third Country:

(a) The parties agree to execute the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") issued by the UK Information Commissioner under Section 119A(1) of the Data Protection Act 2018, as may be amended or replaced from time to time.

(b) The UK Addendum shall be deemed incorporated into this DPA by reference. For purposes of the UK Addendum: (i) Table 1 shall be completed with the parties' details as set forth in the Agreement; (ii) Table 2 shall specify that the Approved EU SCCs referenced are those incorporated under Section 10.2; (iii) Table 3 shall be completed in accordance with Annex 2 to this DPA; and (iv) Table 4 shall specify that neither party may end the UK Addendum as set out in Section 19 of the UK Addendum.

10.4. Alternative Transfer Mechanisms. The Standard Contractual Clauses and UK Addendum will not apply to a Data Transfer if InterWorks has adopted Binding Corporate Rules for Processors approved by a competent supervisory authority, or if another lawful transfer mechanism recognized under applicable Data Protection Laws is in place.

10.5. Transfer Impact Assessments. Upon Customer's reasonable request, InterWorks will cooperate with Customer in conducting transfer impact assessments and implementing supplementary measures as may be required to ensure an adequate level of protection for Customer Data transferred to Third Countries.

10.6. Data Localization. Upon Customer's written request and subject to additional fees, InterWorks will ensure that Customer Data is processed and stored only within specified geographic regions. Such data localization requirements shall be documented in the applicable Ordering Document.

10.7. Government Access Requests. If InterWorks receives a legally binding request from a government authority for access to Customer Data, InterWorks will:

(a) Notify Customer of the request before disclosure (unless legally prohibited);
(b) Challenge the request if there are reasonable grounds to consider it unlawful;
(c) Exhaust available appeals before disclosing Customer Data; and
(d) Provide the minimum amount of information necessary to comply with the request.

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, as applicable: (a) 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 (the "EU GDPR"); and (b) the EU GDPR as incorporated into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and

Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (the "UK GDPR"). References to "GDPR" shall be construed as references to the EU GDPR and/or UK GDPR as applicable to the processing of Customer Data.

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).

15.14. "Data Protection Laws" means all applicable laws and regulations relating to the processing of personal data and privacy, including the EU GDPR, UK GDPR, Australian Privacy Law, Singapore PDPA, U.S. State Privacy Laws, Canadian Privacy Laws, and any implementing legislation, as amended from time to time.

15.15. "Australian Privacy Law" means the Privacy Act 1988 (Cth) and the Australian Privacy Principles contained in Schedule 1 thereto.

15.16. "Singapore PDPA" means the Personal Data Protection Act 2012 of Singapore.

15.17. "U.S. State Privacy Laws" means the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 et seq.), the Virginia Consumer Data Protection Act (Va. Code Ann. § 59.1-575 et seq.), the Colorado Privacy Act (Colo. Rev. Stat. § 6-1-1301 et seq.), the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and any other U.S. state law that imposes obligations on processors or service providers of personal data substantially similar to those imposed by the foregoing laws.

15.18. "Canadian Privacy Laws" means the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) ("PIPEDA"), the Act Respecting the Protection of Personal Information in the Private Sector (Quebec), and any substantially similar provincial privacy legislation.

16. U.S. State Privacy Laws

This Section 16 applies to the extent that U.S. State Privacy Laws govern the processing of Customer Data.

16.1. Role of InterWorks. For purposes of U.S. State Privacy Laws, InterWorks is a "service provider" (as defined in CCPA/CPRA) or "processor" (as defined in other U.S. State Privacy Laws) that processes Customer Data on behalf of Customer.

16.2. Processing Limitations. InterWorks shall:
(a) Process Customer Data only for the specific business purposes set forth in this Agreement, or as otherwise permitted by U.S. State Privacy Laws for service providers or processors;
(b) Not "sell" or "share" Customer Data (as those terms are defined in CCPA/CPRA) or process Customer Data for purposes of targeted advertising or cross-context behavioral advertising;
(c) Not combine Customer Data with personal information received from other sources, except as permitted by U.S. State Privacy Laws;
(d) Provide the same level of privacy protection as required by U.S. State Privacy Laws;

(e) Notify Customer if InterWorks determines it can no longer meet its obligations under U.S. State Privacy Laws; and
(f) Allow Customer to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Data.

16.3. Consumer Rights Requests. InterWorks will assist Customer in responding to verifiable consumer requests to exercise rights under U.S. State Privacy Laws (including rights to access, delete, correct, and opt-out) by providing Customer with the ability to access, delete, or export Customer Data, or by other reasonable means.

16.4. Subcontractor Flow-Down. InterWorks will ensure that any subcontractor engaged to process Customer Data on InterWorks' behalf is contractually obligated to meet the requirements of this Section 16.

16.5. Certification. InterWorks certifies that it understands and will comply with the restrictions and obligations set forth in this Section 16 and applicable U.S. State Privacy Law.

17. Australian Privacy Law

This Section 17 applies to the extent that Australian Privacy Law governs the processing of Customer Data.

17.1. Australian Privacy Principles. InterWorks will process Customer Data in accordance with the Australian Privacy Principles to the extent applicable to InterWorks as a recipient of personal information from Customer.

17.2. Cross-Border Disclosure. Before disclosing Customer Data to a recipient outside Australia, InterWorks will take reasonable steps to ensure that the recipient does not breach the Australian Privacy Principles in relation to that information, except where:
(a) InterWorks reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to the Australian Privacy Principles, and there are mechanisms available to the individual to enforce that protection;
(b) The individual consents to the disclosure after being expressly informed that the Australian Privacy Principles will not apply; or
(c) The disclosure is required or authorized by Australian law.

17.3. Notifiable Data Breaches. InterWorks will notify Customer without undue delay upon becoming aware of an "eligible data breach" (as defined in the Privacy Act 1988) affecting Customer Data, and will provide Customer with information reasonably necessary for Customer to assess and respond to the breach, including for purposes of notification to the Office of the Australian Information Commissioner and affected individuals.

17.4. Access and Correction. InterWorks will assist Customer in responding to requests from individuals to access or correct their personal information in accordance with Australian Privacy Principles 12 and 13.

18. Singapore Personal Data Protection Act

This Section 18 applies to the extent that the Singapore PDPA governs the processing of Customer Data.

18.1. Data Intermediary Obligations. For purposes of the Singapore PDPA, InterWorks acts as a "data intermediary" processing Customer Data on behalf of Customer. InterWorks will:
(a) Process Customer Data only for purposes specified by Customer and in accordance with Customer's instructions;
(b) Implement reasonable security arrangements to protect Customer Data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks;
(c) Cease retention of Customer Data as soon as it is reasonable to assume that the purpose for which the data was collected is no longer being served and retention is no longer necessary for legal or business purposes; and
(d) Not transfer Customer Data outside Singapore except in accordance with the requirements of the Singapore PDPA.

18.2. Data Breach Notification. InterWorks will notify Customer without undue delay upon becoming aware of a data breach affecting Customer Data that is likely to result in significant harm to affected individuals or is of a significant scale, and will provide Customer with information reasonably necessary for Customer to assess and respond to the breach, including for purposes of notification to the Personal Data Protection Commission.

18.3. Access and Correction. InterWorks will assist Customer in responding to access and correction requests from individuals in accordance with the Singapore PDPA.

19. Canadian Privacy Laws

This Section 19 applies to the extent that Canadian Privacy Laws govern the processing of Customer Data.

19.1. PIPEDA Compliance. InterWorks will process Customer Data in accordance with the principles set out in Schedule 1 to PIPEDA (the CSA Model Code for the Protection of Personal Information) to the extent applicable.

19.2. Quebec Law 25. To the extent Quebec's Act Respecting the Protection of Personal Information in the Private Sector applies:

(a) InterWorks will implement security measures appropriate to the sensitivity of the Customer Data;
(b) InterWorks will notify Customer without undue delay of any confidentiality incident involving Customer Data that presents a risk of serious injury to the individuals concerned;
(c) Before transferring Customer Data outside Quebec, InterWorks will conduct a privacy impact assessment and ensure that the data will benefit from adequate protection; and
(d) InterWorks will assist Customer in responding to requests from individuals to exercise their rights under Quebec privacy law, including rights of access, rectification, and de-indexing.

19.3. Cross-Border Transfers. InterWorks will ensure that any transfer of Customer Data outside Canada is made in accordance with applicable Canadian Privacy Laws and that the recipient provides a comparable level of protection.

20. Data Protection Contacts

20.1. InterWorks Privacy Contact. InterWorks has designated a privacy contact who can be reached at privacy@interworks.com for inquiries regarding this DPA and InterWorks' data protection practices.

20.2. Data Protection Officer. To the extent required by applicable Data Protection Laws, InterWorks will appoint a Data Protection Officer and provide Customer with the DPO's contact details upon request.

20.3. Customer Contact. Customer will designate a contact for data protection matters and provide InterWorks with current contact information for purposes of notifications under this DPA.

JURISDICTION-SPECIFIC SCHEDULES

SCHEDULE 1: UNITED KINGDOM DATA PROTECTION

This Schedule applies when UK GDPR governs the processing of Customer Data.

1. UK GDPR Application. References to "GDPR" in this DPA shall include the UK GDPR. References to "supervisory authority" shall include the UK Information Commissioner's Office.

2. UK International Data Transfer Addendum. For transfers of Customer Data from the United Kingdom to countries not subject to an adequacy decision under UK law, the parties agree that the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022) is incorporated into this DPA by reference.

3. UK Addendum Tables. For purposes of the UK Addendum:

Table	Completion
Table 1 (Parties)	As set forth in the Agreement
Table 2 (Selected SCCs)	The Approved EU SCCs incorporated under Section 10.2 of this DPA, including the Appendix Information
Table 3 (Appendix Information)	As set forth in Section 1.2 of this DPA
Table 4 (Ending the Addendum)	Neither party may end this Addendum

4. Conflicts. In the event of any conflict between this Schedule and the main body of the DPA with respect to Customer Data subject to UK GDPR, this Schedule shall prevail.

SCHEDULE 2: AUSTRALIA DATA PROTECTION

This Schedule applies when Australian Privacy Law governs the processing of Customer Data.

1. Definitions. For purposes of this Schedule:
   (a) "APP" means the Australian Privacy Principles contained in Schedule 1 to the Privacy Act 1988 (Cth).
   (b) "Eligible Data Breach" has the meaning given in section 26WE of the Privacy Act 1988.
   (c) "OAIC" means the Office of the Australian Information Commissioner.

2. APP Compliance. InterWorks will handle Customer Data in a manner consistent with the APPs, including:
   (a) APP 6 (Use or Disclosure): Processing Customer Data only for the purposes for which it was collected or a directly related secondary purpose;
   (b) APP 8 (Cross-Border Disclosure): Ensuring overseas recipients of Customer Data are bound by obligations substantially similar to the APPs;
   (c) APP 11 (Security): Taking reasonable steps to protect Customer Data from misuse, interference, loss, and unauthorized access, modification, or disclosure.

3. Notifiable Data Breaches Scheme. If InterWorks becomes aware of an Eligible Data Breach affecting Customer Data:
   (a) InterWorks will notify Customer within 24 hours of becoming aware of the breach;
   (b) InterWorks will provide Customer with all information reasonably necessary for Customer to assess the breach and comply with notification obligations to the OAIC and affected individuals;
   (c) InterWorks will cooperate with Customer's investigation and remediation efforts.

4. Consumer Data Right. If Customer Data includes "CDR data" subject to the Consumer Data Right regime, InterWorks will comply with the applicable data standards and privacy safeguards.

5. Governing Law. Notwithstanding any choice of law provision in the Agreement, this Schedule shall be governed by the laws of the Commonwealth of Australia and the State of New South Wales.

SCHEDULE 3: SINGAPORE DATA PROTECTION

This Schedule applies when the Singapore PDPA governs the processing of Customer Data.

1. Definitions. For purposes of this Schedule:
   (a) "PDPA" means the Personal Data Protection Act 2012 of Singapore.
   (b) "PDPC" means the Personal Data Protection Commission of Singapore.

2. Data Intermediary Status. InterWorks processes Customer Data as a "data intermediary" under the PDPA. InterWorks will:
   (a) Process Customer Data only in accordance with Customer's written instructions;
   (b) Implement security arrangements that are reasonable and appropriate to prevent unauthorized access, collection, use, disclosure, copying, modification, or disposal of Customer Data;
   (c) Develop and implement policies and practices to meet PDPA obligations, including a data protection policy and complaint-handling process.

3. Data Breach Notification. InterWorks will notify Customer of a data breach affecting Customer Data:
   (a) Within 24 hours if the breach is likely to result in significant harm to affected individuals or is of a significant scale (affecting 500 or more individuals); or
   (b) Within 72 hours for other notifiable breaches.

InterWorks will provide sufficient information for Customer to assess whether notification to the PDPC is required within the statutory timeframe.

4. Cross-Border Transfers. Before transferring Customer Data outside Singapore, InterWorks will ensure that the recipient is bound by legally enforceable obligations to provide a standard of protection comparable to that under the PDPA, or that another exception under the PDPA applies.

5. Retention. InterWorks will cease to retain Customer Data as soon as it is reasonable to assume that the purpose for which the data was collected is no longer being served and retention is no longer necessary for legal or business purposes.

SCHEDULE 4: U.S. STATE PRIVACY LAWS

This Schedule applies when U.S. State Privacy Laws govern the processing of Customer Data.

1. CCPA/CPRA Specific Terms. To the extent the California Consumer Privacy Act applies:
   (a) InterWorks is a "service provider" as defined in Cal. Civ. Code § 1798.140(ag).
   (b) InterWorks will not: Sell or share Customer Data; Retain, use, or disclose Customer Data for any purpose other than the business purposes specified in the Agreement, including for a commercial purpose other than providing the Services; Retain, use, or disclose Customer Data outside the direct business relationship between InterWorks and Customer; Combine Customer Data with personal information received from other sources, except as permitted by CCPA/CPRA.
   (c) InterWorks certifies that it understands and will comply with these restrictions.
   (d) Customer has the right to take reasonable and appropriate steps to ensure InterWorks uses Customer Data in a manner consistent with Customer's obligations under CCPA/CPRA.
   (e) InterWorks will notify Customer if it determines it can no longer meet its obligations under CCPA/CPRA.

2. Other State Laws. For purposes of the Virginia CDPA, Colorado CPA, Connecticut CDPA, Utah UCPA, and similar state laws, InterWorks is a "processor" and will:
   (a) Adhere to Customer's instructions and assist Customer in meeting its obligations under applicable law;
   (b) Ensure each person processing Customer Data is subject to a duty of confidentiality;
   (c) Delete or return Customer Data at Customer's direction at the end of the Services;
   (d) Make available information necessary to demonstrate compliance upon reasonable request;

(e) Allow and cooperate with reasonable assessments by Customer or Customer's designated assessor.

3. Consumer Rights. InterWorks will assist Customer in responding to consumer rights requests, including requests to: (a) Access personal information; (b) Delete personal information; (c) Correct inaccurate personal information; (d) Obtain a portable copy of personal information; (e) Opt out of sales, sharing, or targeted advertising.

SCHEDULE 5: CANADIAN PRIVACY LAWS

This Schedule applies when Canadian Privacy Laws govern the processing of Customer Data.

1. PIPEDA Compliance. InterWorks will process Customer Data in accordance with the fair information principles in Schedule 1 to PIPEDA, including:

(a) Accountability for Customer Data in InterWorks' possession or custody;
(b) Limiting collection, use, and disclosure to purposes identified by Customer;
(c) Implementing security safeguards appropriate to the sensitivity of Customer Data;
(d) Providing individuals with access to their personal information upon Customer's request.

2. Quebec Law 25 Compliance. To the extent Quebec's privacy law applies:

(a) InterWorks will implement security measures appropriate to the sensitivity of Customer Data, the purposes for which it is used, and the quantity and distribution of the data;
(b) InterWorks will notify Customer of any "confidentiality incident" (incident de confidentialité) involving Customer Data that presents a risk of serious injury within 24 hours of becoming aware of the incident;
(c) InterWorks will cooperate with Customer in conducting privacy impact assessments for cross-border transfers;
(d) InterWorks will assist Customer in responding to requests for access, rectification, cessation of dissemination, and de-indexing.

3. Breach Notification. InterWorks will notify Customer of any breach of security safeguards involving Customer Data that creates a real risk of significant harm to individuals, and will provide information necessary for Customer to assess and report the breach to the Office of the Privacy Commissioner of Canada.

4. Language. For engagements with Quebec-based customers, InterWorks will provide this Schedule in French upon request.

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.
(a) 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.
(b) 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.
(c) 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.