INTERSYSTEMS CLOUD
DATA PROCESSING TERMS & CONDITIONS

Beginning on the Effective Date and continuing throughout the Term of your Agreement or relevant SOW, InterSystems shall provide the InterSystems Cloud ("your Services") in accordance with these Data Processing Terms & Conditions ("DPA"). InterSystems and Customer are parties to this DPA (each separately "a Party", altogether "Parties").

In consideration of the mutual covenants and promises contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged by the Parties hereto, the Parties agree as follows:

All capitalized terms used in this DPA and not defined elsewhere herein or in your Agreement shall have the same meaning as those terms as used or defined in the GDPR, as defined below. The terms of this DPA supersede any conflicting terms of your Agreement in such a manner to permit the Parties to comply with Data Protection Law, as defined below.

The Parties acknowledge that the services provided by InterSystems under your Agreement are not intended to result in InterSystems creating, receiving, maintaining, transmitting, using, disclosing or otherwise Processing Personal Data related to a Data Subject in an operational context that constitutes Customer Data, as defined below; however, because the Customer, under certain circumstances, may be required to comply with Data Protection Law, as defined below, Customer requires its service providers that may come into contact with Customer Data to enter into a data processing agreement with Customer and InterSystems is willing to enter into such an agreement related specifically to the processing of personal data as referenced in your Agreement, but without conceding that InterSystems is generally a data processor as defined by data protection laws, including, but not limited to the GDPR, as defined below. The Parties agree with regard to other Personal Data Processed by InterSystems that is not Customer Data ("InterSystems Data") that InterSystems is the Data Controller and that the Parties are not Joint Controllers of InterSystems Data.

1. Definitions.

1.1. In this DPA, the expressions "personal data", "data controller", "data processor", "processing" and "process" shall have the meanings assigned to them by the General Data Protection Regulation, Regulation (EU) 2016/679, save that the expression "personal data" as used in this DPA shall refer solely to personal data of which Customer is the data controller or data processor and which InterSystems is processing on behalf of Customer in terms of this DPA.

1.2. Controller's Data. "Controller's Data" means any personal data provided by or on behalf of Customer for processing by InterSystems.

1.3. Customer Data. "Customer Data" means any Personal Data for which Customer or, if Customer is a Data Processor for a Data Controller, the Data Controller solely determines the purposes and means of the Processing of such Personal Data and is provided by or on behalf of Customer to InterSystems; provided that Customer Data shall not include any Personal Data defined as InterSystems Data above.

1.4. Data Controller. "Data Controller" means, when used in reference in this DPA, to refer to Customer or, if Customer is a data processor, the data controller for which Customer processes the personal data.

1.5. Data Owner. "Data Owner" means, with respect to each item of personal data, Customer or, if Customer has contracted with a third party in relation to the personal data, such third party.

1.6. Data Processor. "Data Processor" means, when used as a reference in this DPA, to refer to InterSystems when acting in a capacity as a data processor of Customer and not otherwise acting as a service provider or third party vendor to the Customer.

1.7. Data Protection Law. "Data Protection Law" means all applicable laws or regulations in connection with privacy and the processing, collection, use, and protection of Personal Data in any jurisdiction applicable to your Agreement or the Customer Data, which may include the Data Protection Act 2018 (UK), GDPR, Gramm-Leach-Bliley Act (US), Privacy Act (AU), Privacy Act 1993 (NZ).

1.8. Global Privacy and Security Specification. "Global Privacy and Security Specification" means the InterSystems Global Privacy and Security Specification document, found at www.intersystems.com/MSGPSS, as it may be amended and updated from time to time.

1.9. GDPR. "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679).

INTERSYSTEMS CLOUD
DATA PROCESSING TERMS & CONDITIONS

2. Data Ownership.

2.1. Personal data, which the Data Processor processes on behalf of the Customer will at all times remain the property of the Data Owner.

2.2. Should any party for any reason terminate a contract relating to personal data, the Data Owner of such personal data will decide whether each item of information will be returned to the Data Owner or deleted. All processing by the Data Processor will end except for any processing required by law or which is necessary to bring the relevant contract to an end.

2.3. The Customer may at any time require the Data Processor to stop processing personal data of which Customer is the Data Owner or data processor for Data Controller and to delete and return them to the Customer.

2.4. In the event Data Processor determines that returning or destroying the personal data as required above is infeasible, Data Processor shall extend the protections of this DPA to such personal data, and shall limit further processing of such personal data, to those purposes that make the return or destruction infeasible, for so long as Data Processor maintains such personal data.

3. Obligations and Activities of Data Processor.

3.1. Data Processor agrees to process Controller's Data subject to technical and organisational security measures as provided for in the Global Privacy and Security Specification.

3.2. Data Processor agrees it will process such data only in accordance with instructions from Customer that Customer shall provide in writing from time to time.

3.3. Data Processor agrees, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate under your Agreement and with regard to the responsibilities between the Parties:

3.3.1. the pseudonymisation and encryption of Personal Data;

3.3.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3.3.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

3.3.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.4. Data Processor agrees it shall ensure that all members of staff, agents, contractors and others who have access to Customer Data are advised that the data are confidential and not to be disclosed to anyone not subject to an enforceable duty of confidentiality in respect thereof. Only such members who have an operational requirement to access Customer Data shall be authorised and (in terms of logical, physical or other security measures) able to do so.

3.5. In the event the Data Processor wish to sub-contract the processing, they must impose on any sub-contractor the same contractual obligations in respect of security as has been established in terms of this DPA.

3.6. Data Processor agrees to advise the Customer of any security breaches in accordance with the Global Privacy and Security Specification.

3.7. Data Processor agrees to ensure that all staff who are involved in processing of personal data on behalf of the Customer receive the appropriate training in data protection procedures, identify and keep records of training received by such staff and contents of all courses. The Data Processor shall ensure that no other agents or employees of the Data Processor are given access to the Customer Data.

3.8. Data Processor agrees that the Customer Data shall not be transferred to a country or territory outside the Region designated in your Agreement for the Services without the prior written consent of the Data Controller. Without

prejudice to the foregoing requirement, the Customer Data shall not be transferred to any country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data consistent with the Data Protection Law relevant; however, the parties acknowledge that the Customer Data may be transferred, without any implied breach of this provision, where the transferee has entered into an appropriate agreement or covenant, such as the Standard Contractual Clauses, as approved by the European Commission, or has obligated itself to a data protection code of conduct, such as Binding Corporate Rules as approved or accepted by a relevant data protection authority.

4. Obligations of Customer

4.1. Customer shall only provide Customer Data to InterSystems when strictly required for the purposes of your Agreement and in full compliance with the Data Protection Law and agrees to provide only the minimum necessary Personal Data relevant to your Agreement.

4.2. Customer shall not ask or require Data Processor to process Customer Data in a manner in which Customer could not do as a data controller or a data processor for a data controller.

4.3. Customer represents and warrants that it (or in the case that Customer is a data processor, the relevant Data Controller) may process Customer Data in the manner that Data Processor is authorized to process personal data under this DPA.

4.4. Customer shall be responsible for using administrative, physical and technical safeguards at all times to maintain and ensure the confidentiality, privacy and security of Customer Data transmitted to Data Processor in accordance with the standards and requirements of the Data Protection Law, until such Customer Data is received by Data Processor.

4.5. Customer shall obtain any consent or authorization or ensure such are secured by the Data Controller that may be required by applicable law in order for Data Processor to provide the Services under your Agreement.

5. Miscellaneous.

5.1. Changes to this DPA. The Parties agree to negotiate in good faith to amend this DPA or your Agreement as necessary to comply with any changes in the applicable Data Protection Law. If, within sixty (60) calendar days after InterSystems receives a proposed amendment for this purpose from Customer, the Parties are unable in good faith to reach agreement on its terms, either Party may terminate your Agreement and this DPA by written notice to the other.

5.2. Survival. The respective rights and obligations of Data Processor shall survive termination for so long as Data Processor maintains any Customer Data.

5.3. Interpretation. Any ambiguity in this DPA shall be resolved to permit the Parties to comply with the relevant Data Protection Law.

5.4. Remedies. The rights and obligations under this DPA are in addition to, and not instead of, any rights or obligations arising between the parties under any other contract or at common law.

5.5. In the event of a breach or apprehended breach by any person of an obligation of confidentiality which that person owes to any of the Parties hereto in respect of Customer Data which that person has or had access to as a consequence of this DPA, the Party to whom the obligation is owed undertakes to use its best endeavours to enforce the obligation in question.