GDPR Statement

InterSystems endeavours through its Global Trust program to provide appropriate and necessary protections and safeguards during any processing, including the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, of Personal Information. Because InterSystems is a global organisation with the need to permit transfers to non-U.S. locations, InterSystems has chosen to not self-certify to the EU-U.S. Data Protection Framework (DPF), the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. DPF (the "Framework"). Nevertheless, InterSystems is thoroughly committed to the foundation of the Framework's privacy principles. InterSystems demonstrates its commitment by maintaining policies and controls ensuring the legitimate use, proper disclosure, confidentiality, retention, and minimal contact of any Personal Information as defined in and consistent and in compliance with the General Data Protection Regulation ((EU) 2016/679) ("GDPR"). Furthermore, InterSystems demonstrates its commitment by use of the Standard Contractual Clauses—Controller-to-Controller and Processor-to-Processor—and the UK International Data Transfer Addendum.

The following complements our current License Agreement for customers licensed (herein "Customer") to use our HealthShare, TrakCare, and Data Platforms (InterSystems IRIS, IRIS for Health, Caché, and Ensemble) products ("Licensed Product") and who have an active service agreement with InterSystems to provide applicable services ("Service Agreement"), which may also include any implementation services.

Core Processing Provisions

Any processing of Personal Information by InterSystems under a License Agreement or Service Agreement shall relate to Customer's access and use of the Licensed Product and the Personal Information processed through such where the Customer is a data controller (or a data processor for the data controller) and InterSystems shall act as a Data Processor taking on the responsibilities as required under Article 28.

Any processing of Personal Information by InterSystems to provide Product Support, Training, or Billing/Invoicing relating to a Licensed Product or InterSystems technology where InterSystems determines the manner and purpose for the processing of such Personal Information, InterSystems shall act as a Data Controller taking on the responsibilities as required under Article 24.

Any processing of Personal Information by InterSystems is directly related to the purposes of the legitimate interests pursued by the Customer, including:

- Issue investigation and resolution by InterSystems relating to Personal Information, including patient records – where this cannot be performed by the customer itself or without access to the personal information, such as when a user has completed an action in error and wants to undo the transaction or

rectify the result or a user is unable to complete an action due to the operation of the Licensed Product.

- Implementation of a new system or an upgrade to existing system by InterSystems, to include testing that the system is functioning correctly, because behaviours may be specific to existing data rather than new data added.

- Data migration services from InterSystems, either during implementation for the population of a new live environment with data from a legacy system or for a major upgrade where database version compatibility is an issue.
- Interface testing by InterSystems where the external system does not have a test environment to which to connect.
- InterSystems' support of interfaces between clinical systems and disparate operational support systems with patient data.
- InterSystems' support of national reporting – e.g. Commissioning Data Sets.

The duration of any processing of Personal Information by InterSystems shall be for the period of time relevant to the particular purpose for the processing and the delivery of the underlying services to the Customer.

The Personal Information to be processed for such services is:

1. For HealthShare (includes Information Exchange, Personal Community, Health Insight, Patient Index, and Health Connect), patient records containing aggregated information from applicable participants in a healthcare community as designated by the Customer queried from the source systems as required and including data elements from primary or acute settings, allergies, medications, lab results, encounter and episode records, social history, care plans, and general alerts.
2. For TrakCare (includes Patient Administration System Foundation (plus Extensions), Clinical Information System Foundation (plus Extensions), TrakCare Operational Extensions, and TrakCare for Labs), patient records containing episode and care information from the relevant healthcare provider(s) as designated by the Customer representing the patient chart, family and medical history, lab reports and images, prescriptions and medications, vaccinations, clinical notes, care diagnosis, care and appointment communications, contact and billing information, care and medical alerts, demographics, progress notes, problems, medications, vital signs, and administrative data.
3. For Data Platforms (includes InterSystems IRIS, IRIS for Health, Caché, and Ensemble), may include the same data types as for HealthShare and TrakCare, plus any personal data that (i) identifies or can be used to identify, contact or locate an individual, or (ii) that relates to an individual, whose identity can be either directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of any attributes or status of such individual as notified to InterSystems by the Customer.

Our Representations

With regard to Personal Information for which Customer is the data controller, InterSystems will only act on the written instructions of the Customer;

InterSystems will ensure that our personnel processing the Personal Information are subject to a duty of confidence;

InterSystems will take appropriate measures regarding the security of processing, consistent with the descriptions in the Security Safeguards section below and in a manner that takes into account the nature of the data to be protected, harm that might result from a data breach, relevant technology methodologies and developments impacting the Personal Information, and the direct and indirect costs for implementing such controls;

InterSystems will only engage sub-processors with the prior written consent of the Customer and under a written contract with such sub-processors;

InterSystems will assist the Customer in providing subject access and allowing data subjects to exercise their rights under the GDPR, in circumstances where the Customer cannot do so through their access to the Licensed Product;

As applicable, InterSystems will assist the Customer in meeting its GDPR obligations in relation to the security of the processing, the notification of personal data breaches and data protection impact assessments as they relate to any processing of personal information by InterSystems;

InterSystems will delete or return all personal data to the Customer as requested at the end of the contract;

InterSystems will submit to audits and inspections, excepting any such onsite; provided that such do not interfere or impact InterSystems' obligations of confidentiality under law or contract or disrupt its ordinary course of business;

InterSystems will provide the Customer with the applicable information in InterSystems pocession that Customer needs to ensure that InterSystems and Customer are meeting the obligations for a Processor under Article 28;

InterSystems shall maintain, as currently in force and amended, Standard Contractual Clauses, as adapoted by the European Commission, between InterSystems EU entities, as data exporters, and InterSystems non-EU entities, as data importers, to address an necessary and proper transfers of personal information consistent with Article 46;

InterSystems will notify the Customer promptly if InterSystems is asked by the Customer to do something infringing the GDPR or other data protection law of the EU or a member state; and

InterSystems shall appoint a Data Protection Officer consistent with Article 37 and designate that Ken Mortensen shall serve in that role on behalf of InterSystems and all of its affiliates and branch offices around the world with the authority to take any and all actions in connection with data protection matters, including privacy and security.

InterSystems Corporation
One Memorial Drive
Cambridge, MA 02142-1356

Main: +1 617 621 0600
Support: +1 617 621 0700
InterSystems.com

Protections and Safeguards

InterSystems commits to its Global Trust program by providing appropriate and necessary protections and safeguards to ensure the legitimate use, proper disclosure, and minimal contact of any Personal Information, which, for InterSystems, encompasses the legal and regulatory definitions of personal data, whether InterSystems is a Covered Business, Personal Information Processor, Data Controller, Data Processor, Business Associate, or Covered Entity, to include any and all information or data (regardless of format) that (i) identifies or can be used to identify, contact or locate an individual, or (ii) that relates to an individual, whose identity can be either directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of any attributes or status of such individual.

Our Global Trust Data Protection, Privacy & Security Policy uses a framework of controls based on ISO, HIPAA, NIST, APEC CBPR, and EU DPD/GDPR requirements. InterSystems designs and uses controls relevant to manage the confidentiality, integrity, and availability of Personal Information using the ISO 27001/2 standard so that the specific privacy, security, and business objectives of InterSystems and our customers are met. InterSystems takes a holistic, coordinated view of the privacy and security risks in order to implement a comprehensive suite of controls and measures under the overall framework of a coherent management system.

Customer Obligations

Customer shall abide by the InterSystems Information Sharing Terms to ensure appropriate and necessary protections and safeguards of Personal Information in the Customer's interactions with InterSystems, including the Customer providing a fill out Rules of Engagement form under the End User Data Processing Agreement to make InterSystems properly aware of any Personal Information from the Customer to be shared with and used by InterSystems.

Customer will only provide Personal Information to InterSystems when strictly required for the purposes of the License and Service Agreement and in full compliance with the GDPR and applicable data protection law;

Customer will provide only the minimum necessary Personal Information relevant to the License and Service Agreement and the specific services carried out by InterSystems at any time under the License and Service Agreement;

Customer will not ask or require InterSystems to process Personal Information in a manner in which the Customer could not do as a data controller or a data processor for another data controller or otherwise in a manner inconsistent with GDPR or other applicable law;

Customer represents and warrants that it (or in the case the Customer is a data processor, the relevant data controller) may process Personal Information in the manner InterSystems is authorized to process Personal Information under the License and Service Agreement;

Customer will be responsible for using administrative, physical and technical safeguards at all times to maintain and ensure the confidentiality, privacy and security of Personal Information transmitted to InterSystems in accordance with the standards and requirements of the GDPR, until such Personal Information is received by InterSystems; and

Customer will obtain any consent or authorization that may be required by the GDPR or applicable law in order for InterSystems to provide its services under the License and Service Agreement.

InterSystems Data Protection Officer

InterSystems has appointed a Data Protection Officer with authority for all data protection matters

Name: Ken Mortensen

Email: dpo@intersystems.com

Phone: +1 (617) 621-0600 (main support); +44 (0)1753 855450 (See Worldwide Offices)

Post: CH: InterSystems B.V., Zweigniederlassung Zürich, c/o Caminada Treuhand AG Zürich, Zollikerstrasse 27, 8008 Zürich
CZ: InterSystems B.V., Slepá II 1007/15, 142 00 Praha 4 – Lhotka
FI: InterSystems B.V. Regus Life Science Center, Keilaranta 16, 5th floor, 02150 Espoo
FR: InterSystems SAS, Tour EuroPlaza, La Défense 4, 20 avenue André Prothin, 92400, Courbevoie
DE: InterSystems GmbH, Robert-Bosch-Str. 16 a, 64293 Darmstadt
IT: InterSystems Italia s.r.l., Centro Leoni, Building A, 5th floor, Via Giovanni Spadolini, 5, 20141 Milano
NL: InterSystems B.V. Regus Utrecht Papendorp, Papendorpseweg 100, Utrecht 3528 BJ
SE: InterSystems Sweden AB, Mäster Samuelsgatan 60, SE-111 21 Stockholm
UK: InterSystems House, Tangier Lane, Eton, Windsor, Berkshire, SL4 6BB England
US: InterSystems Corporation, 1 Congress St., Suite 3200, Boston, MA 02114

Message: Contact Us Form, www.intersystems.com/who-we-are/contact-us/