InterSystems
Health | Business | Government

InterSystems Corporation
One Memorial Drive
Cambridge, MA 02142-1356

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

WHITE PAPER – 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. InterSystems maintains policies and controls to ensure 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").

The following supplements our current License Agreement for customers licensed (herein "Licensee") to use our HealthShare, TrakCare, and Data Platforms (InterSystems IRIS, Caché, and Ensemble) products ("Licensed Product") and who have an active service agreement with InterSystems to provide applicable services ("Service Agreement").

Core Processing Provisions

Any processing of Personal Information by InterSystems under the License and Service Agreement shall relate to Licensee's access and use of the Licensed Product and the Personal Information processed through such.

Any processing of Personal Information by InterSystems is directly related to the purposes of the legitimate interests pursued by the Licensee, 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 Licensee.

The Personal Information to be processed for such services is:

1. For HealthShare, patient records containing aggregated information from applicable participants in a healthcare community as designated by the Licensee 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, patient records containing episode and care information from the relevant healthcare provider(s) as designated by the Licensee 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 (InterSystems IRIS, 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 Licensee.

Our Representations

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

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;

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

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

As applicable, InterSystems will assist the Licensee in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

InterSystems will delete or return all personal data to the Licensee 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 Licensee with the applicable information in InterSystems pocession that Licensee needs to ensure that InterSystems and Licensee are meeting the obligations for a Processor under Article 28; and

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

Security Safeguards

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.

- **Policies and Procedures:** To ensure consistent and comprehensive application of the appropriate and necessary controls and measures, InterSystems documents its privacy and security processes through policies, procedures, standards, work instructions, guidance, and other means.
- **Organization:** To maintain appropriate accountability, InterSystems assigns personnel and third parties to roles that support the functional attributes of Global Trust though privacy and security activities.
- **Human Resources:** To promote understanding by InterSystems employees and contractors that have access to InterSystems' informational assets, including customer data and Personal Information, InterSystems administers these employees and contractors throughout their lifecycle with InterSystems regarding their responsibilities as well as suitability for the roles for which they are considered.
- **Asset Management:** To ensure InterSystems identifies organizational assets and defines appropriate protection responsibilities, InterSystems maintains assets in a manner to ensure that information receives an appropriate level of protection in accordance with its importance to InterSystems and our customers.

- **Access Control:** To limit access as appropriate and necessary to information assets, InterSystems manages authorized user access to provide accountability of InterSystems employees and contractors in order to prevent unauthorized access to systems and services.
- **Cryptography:** To implement cryptographic controls protecting the confidentiality, authenticity, and/or integrity of information, InterSystems deploys industry standard encryption technology.
- **Physical and Environmental:** To define secure areas for the prevention of unauthorized physical access, damage and interference to information and information processing facilities, InterSystems facilitates the protection of assets against loss, damage, theft or compromise of assets, and interruption to operations.
- **Operations:** To operate systems and facilities in a secure manner protecting against malware, conducting regular data backups to protect against loss of data, logging and monitoring to record events and generate evidence, InterSystems manages operational software to confirm the integrity of operational systems, mitigating technical vulnerabilities as discovered, and reviewing information system audit rules to minimize the impact of audit activities on operational systems.
- **Communications and Networks:** To manage network security for the protection of information in networks and InterSystems information processing facilities, InterSystems maintains the security of information transferred both within InterSystems, to/from customers, and with any third party.
- **Acquisition, Development, and Maintenance:** To implement security requirements as an integral part of information systems across the entire lifecycle, including those that provide services over public networks, InterSystems supports development and support processes that design those requirements as part of the lifecycle of our products and systems.
- **Third Parties:** To address information security in our relationships with vendors, suppliers, and other third parties for the protection of information assets, InterSystems conducts a third party risk management assessments.
- **Incident Response:** To respond to information security incidents consistently and effectively to address security events and weaknesses as well as mitigate risks to information assets, including customer data and Personal Information, InterSystems maintains an incident response plan and process.
- **Business Continuity:** To ensure effective availability and integrity of information assets, InterSystems embeds continuity of operations into its functions and systems.

- **Risk and Compliance:** To review ongoing compliance to avoid breaches of legal, statutory, regulatory or contractual obligations, InterSystems performs information security assessments against InterSystems policies and procedures of implemented and operating controls and measures for information security.

Licensee Obligations

Licensee 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;

Licensee 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;

Licensee will not ask or require InterSystems to process Personal Information in a manner in which the Licensee 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;

Licensee represents and warrants that it (or in the case the Licensee 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;

Licensee 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,

Licensee 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

Name: Ken Mortensen

Email: dpo@intersystems.com

Phone: +1 (617) 621-0600 (main support); +44 (0)1753 855450 (EU local number)

Post: InterSystems House, Tangier Lane, Eton, Windsor, Berkshire, SL4 6BB England
One Memorial Drive, Cambridge MA 02142 USA

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