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 – Data Protection, Privacy & Security

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 Data Controller or Data Processor, 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 program uses a framework of controls based on ISO, HIPAA, NIST, APEC CBPR, and EU DPD/GDPR requirements. In order to support Global Trust we (1) identify the specific purposes for which we may need to collect, use, or disclose Personal Information, (2) operationalize protections surrounding Personal Information relating to the privacy rights of individuals while ensuring availability for proper and authorized uses and disclosures, (3) implement safeguards to secure the confidentiality, integrity, and availability of Personal Information in our environments, (4) address education and awareness through a comprehensive Global Trust training initiative, and (5) respond promptly to any actual or suspected threats or vulnerabilities affecting Personal Information.

This briefing paper highlights more specifics of our data protection practices as they pertain to the InterSystems products and services.

Purposes

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

- Issue investigation and resolution relating to personal information or personal data, including patient records – where this cannot be performed by the local organisation support 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 application error.
- Implementation of a new system or an upgrade to existing system, 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, 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 where the external system does not have a test environment to which to connect.
- Support of interfaces between clinical systems and disparate operational support systems with patient data.
- Support of national reporting – e.g. Commissioning Data Sets.

Data Protection and Privacy

InterSystems incorporates and harmonizes the requirements of privacy and data protection legislation and regulation related to the collection, use, and disclosure of Personal Information through the implementation of Global Trust policies and procedures, training on support and operational practices, and controls and measures focused on the relevant protections.

- **Data Protection Officer – Ken Mortensen:** To oversee the accountability of InterSystems in delivering on its promises for data protection.

  InterSystems appointed a privacy and security professional with an IT and legal background to serve as the global Data Protection Officer for the company.

- **Fair Processing:** To assist our customers in carrying out their mission and objectives through our delivery, support, and maintenance of information systems and processes that collect, use, and disclose Personal Information.

  InterSystems educates our customers on the times and scenarios we need information to make sure that Personal Information is processed only in connection with our services.

- **Lawful Purposes:** To ensure our collection, use, and disclosure of Personal Information links to our support of our customers as data controllers.

  InterSystems uses contracts and procedures with our customers to links any processing of Personal Information to the purposes relevant to the services or support we provide.

- **Minimum Necessary:** To make sure that InterSystems collection, use, and disclosure of Personal Information is adequate, relevant and not excessive.

  InterSystems examines incoming data for Personal Information to ensure receipt only that information relevant and related to the services or support delivered.

- **Data Integrity:** To address the accuracy of Personal Information that is collected, used, and disclosed.

  InterSystems employs its technology to make certain that data, including Personal Information, maintains integrity through our processing while providing our services or support.

- **Limited Retention:** To maintain Personal Information for only as long as appropriate and necessary to address the needs of our customers.

  InterSystems actively uses procedures to remove or to destroy any Personal Information once it is no longer needed to deliver our services or support.

- **Rights of Subjects:** To coordinate with our customers for any responses or inquiries regarding the processing of Personal Information as well as designing solutions permitting effective and efficient accessibility and portability of Personal Information within our products.

  InterSystems communicates with our customers to establish links with their data protection and security personnel to connect any data subject requests back to our customers in a timely and documented fashion.

- **Technical and Organisational Measures:** To put in place controls designed to protect privacy and safeguard Personal Information that InterSystems collects, uses, and discloses.

  InterSystems establishes controls for appropriate and necessary safeguards based upon recognized standards, such as ISO 27000 series and HITRUST, and industry best practices.

- **Data Transfer:** To provide appropriate assurances regarding data protection requirements related to any internal sharing or external disclosures outside the country of origin for the Personal Information.

  InterSystems put in place an internal data transfer agreement between its European entities and its non-European entities, such as in the U.S. and Australia, to obligate the entire organization to privacy and security goals consistent with European data protection laws.

Security Safeguards

InterSystems designs and uses controls relevant to ensure the confidentiality, integrity, and availability of Personal Information using the ISO 27001/2 standard to ensure 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, throughout their lifecycle with InterSystems of their responsibilities as well as to ensure suitability for the roles for which InterSystems employees and contractors are considered.
- **Asset Management:** To ensure InterSystems identifies organizational assets and defines appropriate protection responsibilities as well as 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 through the management of authorized user access with accountability of InterSystems employees and contractors to prevent unauthorized access to systems and services.
- **Cryptography:** To implement cryptographic controls protecting the confidentiality, authenticity, and/or integrity of information.
- **Physical and Environmental:** To define secure areas for the prevention of unauthorized physical access, damage and interference to the organization's information and information processing facilities and to facilitate 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. Managing 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 and

to maintain 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, and in our development and support processes to 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.
- **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.
- **Business Continuity:** To embed continuity of operations ensuring effective availability and integrity of information assets.
- **Risk and Compliance:** To review ongoing compliance to avoid breaches of legal, statutory, regulatory or contractual obligations through information security assessments against InterSystems policies and procedures of implemented and operating controls and measures for information security.

Training

- Data protection training is provided to each new InterSystems Personnel in the form of confirmed review of policies and procedures.
- All InterSystems Personnel must review data protection policies annually.
- All InterSystems Personnel supporting our Solution Services receive ITIL training.

Security Incident Response

A security incident is any identified breach of access, data handling, or security policy. When identified, a security incident will be addressed with the highest level of response and will receive continuous effort 24/7 until any data risk is removed.

- All security incidents will be reported to InterSystems Legal Department immediately upon detection. The Legal Department will coordinate communication with the customer.
- The Vice President of Client Services will be informed and will be responsible for InterSystems senior management communication.
- Security incidents will NOT be documented in WRC. This is to ensure that no additional data risk is introduced.

- Disclosure of security incidents related to Managed Services customers will not be made public without specific written authorization from the customer
- Any incident that results in a data breach will follow InterSystems standard data breach procedure.
- For any security incident, the response will prioritize data protection. Managed Services will evaluate the risk and may prioritize data security over system availability.

General Data Protection Regulation

Although our Global Trust program looks to protect Personal Information by addressing global privacy and security requirements, InterSystems privacy and security controls are consistent with the obligations under the EU General Data Protection Regulation (GDPR). As noted above, our current controls ensure consistency across the existing principles for data protection and align with the GDPR and ongoing updates to EU member state legislation. InterSystems undertook several actions, some of which are ongoing – as required under GDPR – to address any new issues, in particular:

1. We have appointed a **Data Protection Officer**, as noted above.
2. We have mapped our personal information processing by identifying, as associated with our customers, what, if any, personal information we collection, use, or disclose.
3. We have prioritized relevant actions that include ongoing assessment of the personal information lifecycle and, through our DPO, ensuring our design processes take into account the risks associated with the privacy of individuals and the security of information.
4. We have processes in place to perform Data Protection Impact Assessments (DPIAs) when necessary to understand what if any risks exist to the rights of individuals are impacted by our processing and to identify appropriate and necessary mitigations to address the recognized risks.
5. We have ongoing organizational activities to organize our internal processes, including new and updated privacy and security policies, ongoing assessment of operational processing to ensure effective controls, new training and awareness on data protection for employees, and enhancements to our vendor program for data protection requirements.
6. We have put in place requirements to document decisions related to data protection so that our actions and processing can be explained and properly understood.

InterSystems uses its Global Trust program to elevate data protection through our relationships with our customers and continuing to build upon the trust that our customers have with us in delivering quality products and effective services.