Data Protection Governance Standard

Global Trust Standards

InterSystems®
Creative data technology

Document details

Title: Data Protection Governance Standard
Service: Implementation Services and Professional Services
Program: Global Trust

Description: This document serves as the standard to define interactions between the Customer and InterSystems during the delivery of implementation services and professional service in order to ensure appropriate and necessary privacy and security controls for data protection related to compliance with applicable data protection laws.

Document ID: GTDPGS
Version: 2.1
Created by: Ken Mortensen, Data Protection Officer

Document controls

Document Modifications			
Version	Date	Description of Change	Modified By
1.0	13-May-19	Creation of standard	Ken Mortensen
1.1	29-Apr-20	Update for Customer VPN requirements	Ken Mortensen
1.2	2-Jun-20	Enhanced project governance	Ken Mortensen
1.3	27-Apr-21	Clarifications; website publication	Ken Mortensen
1.4	29-Apr-21	Edits to language	Ken Mortensen
2.0	04-Oct-23	Update as a general (all ops) standard	Ken Mortensen
2.1	10-Jun-24	Update to address contacts	Ken Mortensen

Contents

1. Data Protection Governance

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 Confidential Information or Personal Information in the course of providing Implementation or Professional Services to Customers. This document outlines specific governance necessary for any access to Customer data or Customer environment(s) provided by a Customer to InterSystems personnel for purposes of performing implementation or professional services, whether such data or environment(s) are on-premises with the Customer or provided separately by InterSystems through a Managed Service offering.

Note that any contractual requirement to satisfy legal obligations for the protection or safeguarding of Personal Information are addressed in the Implementation Services / Professional Services Business Associate Terms & Conditions (available at https://www.intersystems.com/ISPSBAA) and/or the Implementation Services / Professional Services Data Processing Agreement (available at https://www.intersystems.com/ISPSDPA) when such requirements are incorporated into the services agreement with a Customer. In addition to ensuring observance with the requirements found in this standard, the Customer can find information sharing requirements in the Information Sharing Terms (available at https://www.intersystems.com/ISCIST) as incorporated into the Product Terms related to the products licensed by the Customer.

For InterSystems, Personal Information 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 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 Confidential and 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 Confidential Personal Information.

Our Global Trust program is led by our Data Protection Officer:

- Name: Ken Mortensen
- Email: dpo@intersystems.com
- Phone: +1 (617) 621-0700
+44 (0)1753.855450
- Post: One Congress Street, Boston MA 02114 USA
One Victoria Street, Windsor, Berkshire, SL4 1HB England UK
- Message: Contact Us Form (https://www.intersystems.com/who-we-are/contact-us/)

2. Security Architecture

This document highlights the specifics of the data protection, privacy, and security practices as they pertain to the InterSystems Implementation and Professional Services performed by InterSystems Personnel for a Customer working with Customer data or in the Customer environment.

In order to assure effective data protection controls, InterSystems Personnel, to include employees and contractors, shall not directly access Customer systems from an InterSystems device, such as an assigned laptop, but rather through a bastion host, which is a Customer access server whose purpose to provide access to the Customer's internal environment from an external network. To help protect Customer assets, **InterSystems requires Customer** to permit InterSystems Personnel to go through a Virtual Desktop Interface (VDI) using a "bastion" (or "jump") host to gain functional access to backend systems in protected or sensitive network segments in order to perform necessary implementation and professional services.

A Customer must establish a security architecture for InterSystems's access to Customer's environments supporting the solution to include:

(a) a Customer-provided VPN connection for secure encrypted access by InterSystems to a VDI through a bastion host, which is the only directly accessible system on the VPN segment,

(b) a VDI on a bastion host for accessing systems in the Customer environments supporting the solution,

(c) bastion host end user access configured to allow access to

  (i) only one environment at a time and

  (ii) only to those environments for which the end user requires access

(d) specific technical safeguards on the bastion host to prevent any transfer of personal or confidential information (not including the screen view during access to the bastion host) back to any end user device.

3. Controls and Measures

- Sign off by the Customer Data Protection Officer/Privacy Officer/Information Governance Head regarding:
  a. the design and acceptance of any required security safeguards to be built as part of the requirements for the professional or implementation services and
  b. InterSystems's access to the environment through the security architecture noted above.
- Customer to strictly limit which Customer employees have access to the environments supporting the solution to only those Customer employees with a specific need.
- Customer to document which Customer employees have access (and provide this record to InterSystems as part of the project management documentation) through an appropriate user access review process.
- Customer to document the type and nature of any personal information, especially any sensitive personal information (e.g. health data, Protected Information, Patient Identifiable Data, or clinical records) to be shared with InterSystems prior to any disclosure to or access by InterSystems.
- Customer shall not provide direct accounts for InterSystems Personnel on production instance (e.g. "live" systems).

InterSystems United Kingdom

One Victoria Street
Windsor, Berkshire
SL4 1HB England
Tel: +44.(0)1753.855290

InterSystems.com.uk

InterSystems Australia

Level 12, 383 Kent St
Sydney, NSW
2000 Australia
Tel: +61.2.9380.7111

InterSystems.com.au

InterSystems Corporation
World Headquarters

One Congress Street
Boston, MA 02114
Tel: +1.617.621.0600

InterSystems.com