Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	**3-Aug-22**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	**Full legal name**: UK Establishment of InterSystems Corporation. **Main address**: 70 Tangier Lane, Eton, Windsor, Berkshire SL4 6BB. **Official registration number**: BR000524.	**Full legal name**: InterSystems Non-UK Entities (Annex IV). **Main address**: InterSystems Non-UK Entities c/o InterSystems Corporation, One Memorial Drive, Cambridge, MA 02142 USA.
Key Contact	**Full Name**: Ken Mortensen. **Job Title**: Data Protection Officer. **Contact details including email**: GlobalTrust@InterSystems.com.	**Full Name**: Ken Mortensen. **Job Title**: Data Protection Officer. **Contact details including email**: GlobalTrust@InterSystems.com.
Signature (if required for the purposes of Section 2)	Ken Mortensen 2022.08.24 15:25:59 -04'00'	Ken Mortensen 2022.08.24 15:26:29 -04'00'

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Redress Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Module 1	✓	✓			
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

ANNEX IA: LIST OF PARTIES

Data Exporter(s): UK Establishment of InterSystems Corporation (BR000524).
Role (controller/processor): Controller.

Data Importer(s): InterSystems Non-UK Entities (Annex IV).
Role (controller/processor): Controller.

ANNEX IB: DESCRIPTION OF TRANSFER – HUMAN CAPITAL DATA TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred

The Personal Data transferred concern the following categories of Data Subjects:

1. Employees of the UK Establishment of InterSystems Corporation.
2. Employees of InterSystems assigned or on location of the UK Establishment of InterSystems Corporation.
3. Applicants for employment by the UK Establishment of InterSystems Corporation.

Categories of Personal Data Transferred

The Personal Data transferred concern the following categories of data:

Name, Business and Personal Addresses, National Identification Information (if any), Business and Personal Email addresses, Dependant Information (including names, relationships, gender, birth dates, national identification information), Marital Status, Gender, Birth Date, Business and Personal Telephone Contacts, Job Information (Job Code, compensation, level, supervisor information, location, start date, termination date, job title, FLSA Status, rating scale, manager level, position type, number of direct reports, primary language, student status, education level, residence status, birth country, rating, grade, grade entry date, cost centre, function, subfunction), Employee ID, security video/audio, Payroll data (including banking data necessary to make payments to data subject, compensation information, data on leave, end of service payment and accruals, holiday salary deduction, holiday compensation and accruals, other leave salary deduction); paycheck details (including the following: total gross salary, employee's wage tax (withheld by the employer), employee's compulsory or voluntary deductions, total net salary, overtime compensation, bonus compensation, other variable compensation, other leave compensation, not taken holidays compensation, all company paid expenses, benefits and benefits in kind, housing allowances, travel allowances, staff travel details, car or commuting allowances, other allowances (cost of living, mobile phone, etc.), expenses refund and advances, expatriate expenses refund, benefits in kind deduction, other net adjustments, salary advance adjustments).

Sensitive Data (if applicable)

The Personal Data transferred concern the following categories of sensitive data:

Gender and medical information is transferred for purposes of identification, accommodation (as required by local law), and provision of medical/health insurance (as required locally). Trade-union membership is transferred as necessary to comply with local labour laws and regulations.

Frequency of the Transfer

The data is transferred on a continuous basis.

Nature of the Processing

Employee and applicant information relevant to support the human resource functions and employment of individuals, including any applications and monitoring forms, standard employee records (performance plans/reviews, contacts, and benefit information), payroll, taxation, and financial information.

Purpose(s) of the Data Transfer and Further Processing

The transfer is made for the following purposes:

To perform standard human resource functions, including but not limited to, general human resource operations; management of personnel; training and education programs; strategic planning and operations; corporate security and compliance functions; legal or government imposed requirements; provision of healthcare insurance and appropriate coordination of fringe benefits; training, advice, and counselling purposes, talent management, mentoring, advancement, and succession planning, recruitment, staffing, and talent management; performance management.

Retention Period of Personal Data

Retention of Personal Data is consistent with purpose of transfer and any legal compliance requirements.

Transfers to Sub-Processors

Sub-Processor Name	Subject Matter	Nature	Duration
Workday, Inc.	Enterprise Cloud Management	Employee information relevant to support human resource functions and employment of individuals.	Continuous
Greenhouse, Inc.	Applicant Tracking	Employee application information relevant to support recruiting functions.	Continuous

ANNEX 2B: DESCRIPTION OF TRANSFER – TECHNICAL SERVICES DATA TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred

The Personal Data transferred concern the following categories of Data Subjects:

1. Employees of the Data Exporter.
2. Employees of InterSystems assigned or on location of the UK Establishment of InterSystems Corporation.
3. Employees, agents, and representatives of any supplier of goods and/or services to the Data Exporter.

Categories of Personal Data Transferred

The Personal Data transferred concern the following categories of data:

Name, Business Addresses, Business and (potentially if provided by Data Subject) Personal Email addresses, Calendar schedules, fee/busy indicator, Email header and content information.

Sensitive Data (if applicable)

The Personal Data transferred concern the following categories of sensitive data: None.

Frequency of the Transfer

The data is transferred on a continuous basis.

Nature of the Processing

Technical services data used in the operation of internal support and operational systems, including (1) email, calendar, and contact information used for business purposes within the corporate email system for InterSystems necessary to support business operations and communications, (2) internal systems and server log on information, credentials, and network identification for access and workstation operations necessary for information technology operations, (3) security operations and logical access controls, including logs and audit trails, and (4) help desk tickets to support end users of internal systems and workstations. Other information relevant to support the provision of goods and/or services to the Data Exporter by third party providers.

Purpose(s) of the Data Transfer and Further Processing

The transfer is made for the following purposes:

To permit the operation of internal support and systems, including email, calendar, and contact system, help desk and technical services support, and shared and functional services systems for business operation purposes necessary to support collaboration and communication.

Retention Period of Personal Data

Retention of Personal Data is consistent with purpose of transfer and any legal compliance requirements.

Transfers to Sub-Processors

Sub-Processor Name	Subject Matter	Nature	Duration
Microsoft	Cloud Services	Technical services data used in the operation of internal support and operational systems.	Continuous
ServiceNow, Inc.	Cloud Services	Technical services data used in the operation of internal support and operational systems.	Continuous
iOffice, LP.	Cloud Services	Technical services data used in the operation of internal support and operational systems.	Continuous

ANNEX 3B: DESCRIPTION OF TRANSFER – PRODUCT SUPPORT, IMPLEMENTATION SERVICES, AND MANAGED SERVICES DATA TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred

The Personal Data transferred concern the following categories of Data Subjects:

1. Employees, contractors, business partners, representatives and end customers of Customers, and other individuals whose personal data is collected by or on behalf of Customers and delivered to a Data Importer as part of the InterSystems Services.
2. Employees of InterSystems assigned or on location of the UK Establishment of InterSystems Corporation.
3. Employees, agents, and representatives of any supplier of products and/or services to the Data Exporter.

Categories of Personal Data Transferred

The Personal Data transferred concern the following categories of data:

Data related directly or indirectly to the delivery of InterSystems products and services, including online and offline Customer, prospect, partner and supplier data, and data provided by Customers in connection with the resolution of support requests.

Sensitive Data (if applicable)

The Personal Data transferred concern the following categories of sensitive data:

Customer data about or from Customer end-users or customers revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and data concerning health or sex life, and data relating to offenses, criminal convictions, or security measures.

Frequency of the Transfer

The data is transferred on a continuous basis.

Nature of the Processing

The parties enter into contractual agreements with customers established in the UK (hereinafter the "Customer" or the "Customers") for the provision of InterSystems products and services, including data processing agreements providing the instructions for the receiving party to abide by when processing personal data on behalf of Customer. The personal data transferred will be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between the Data Importer, Data Exporters, and Customers: (a) customer service activities, such as processing orders, providing technical support and improving offerings; (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to Customers, including services offered by means of the products and solutions described at www.cisco.com; and, (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative and regulatory bodies. Other information relevant to support the provision of goods and/or services to the Data Exporter and Data Importer by third party providers.

Purpose(s) of the Data Transfer and Further Processing

The transfer is made for the following purposes:

In providing InterSystems products and services, parties may have access to personal data belonging to Customers' end users and customers and transfer them outside the UK area to a party to make them carry out part of the service.

Retention Period of Personal Data

Retention of Personal Data is consistent with purpose of transfer and any legal compliance requirements.

Transfers to Sub-Processors

Sub-Processor Name	Subject Matter	Nature	Duration
N/A	N/A	N/A	N/A

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer has implemented and will maintain appropriate technical and organisational security measures, internal controls, and information security routines intended to protect personal data, as defined in the InterSystems Data Protection, Privacy, & Security Policy (www.InterSystems.com/GTDPPS) ("the Policy") against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

Amongst the technical and organisational measures specified in the Policy include, but are not limited to:

- Measures ensuring confidentiality, integrity, and availability of asset management based on ISO 27001/2 standard with enhancement through NIST SP 800-53r4.
- Measures ensuring access control consistent with NIST SP 800-63-3.
- Measures ensuring consistent and comprehensive application of policies and procedures.
- Measures ensuring information management security based on ISO 27001/2 and NIST SP 800-53.
- Measures ensuring encryption and protection of data during transmission.
- Measures ensuring events logging and incident response.
- Measures ensuring regular testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure security of processing.
- Measures ensuring protection of data during storage.
- Measures ensuring limited data retention.

Certifications for specific environments, particularly those for maintenance of operational information assets of customers, include:

- Cyber Essentials Plus (Managed Services UK and UK operations),
- HITRUST (Managed Services US),
- ISO 27001 (Managed Services UK and UKI operations), and
- SOC 2/3 (Managed Services US).

ANNEX III: LIST OF SUB PROCESSORS (Modules 2 and 3 only): N/A.

ANNEX IV: LIST OF INTERSYSTEMS NON-UK ENTITIES:

- InterSystems Corporation
- InterSystems Australia PTY Ltd.
- InterSystems do Brasil Ltda.
- InterSystems BV (Israel, Saudi Arabia, South Africa, Switzerland)
- InterSystems BV (Belgium, Czech Republic, Finland, Republic of Ireland)
- InterSystems Colombia SAS
- InterSystems Chile Ltda.
- InterSystems FZ LCC (U.A.E.)
- InterSystems GmbH (Germany)
- InterSystems (Hong Kong) Ltd.
- InterSystems Iberia, S.L. (Spain)
- InterSystems Italia S.R.L. (Italy)
- InterSystems Japan KK
- InterSystems New Zealand, Inc.
- InterSystems SAS (France) 5
- InterSystems Singapore PTE Ltd.
- InterSystems Software (Beijing) Co, Ltd.
- InterSystems Software Thailand Ltd.
- InterSystems Sweden AB (Sweden)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.