qs.com

External

Information and Privacy Security Policy

1 History of versions

Date	Version	Author	Comments
23/01/2019	1.0	Koljonen, Christina	First Release
31/03/2020	2.0	Senthil Kumar C R	I. Accommodated in the QS Unisolution standard template. II. Updated sections: a. Introduction b. Management of Technical vulnerabilities III. Added Revision section
06.11.2020	3.0	Senthil Kumar C R	Formatting of the document and inclusion of GDPR in Section 9.1
27.05.2021	4.0	Senthil Kumar C R	Updates for External Certification Audit 2021
31.08.2021	5.0	Deepali Saxena	QS Rebranding template updated (logo, font etc)
29.03.2022	5.1	Senthil Kumar C R	Mapped to GDPR (EU 2016/679) and European Council, & Commission decision C (2021) 3972 final dated 4.6.2021, included EDPB measures
05.01.2023	5.2	Senthil Kumar C R	Updates for inclusion of PIMS

2 Reference

ISO 27001:2013	ISO 27001:2022	ISO 27701	ISO 27018	GDPR/BDSG
5.2	5.2	5.3.2		GDPR Chapter IV and Chapter V

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

External

Table of contents

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

3 Introduction

This document outlines the information & privacy security policies put in place by senior management of the QS Institution Performance (QSIP) Products MoveON & MoveIN. The IPSMS Policy below is supported by various subordinate policies, procedures, guidelines, templates, and checklists.

QS MoveON & MoveIN IPSMS Policy

We, at QS Institutional Performance shall continuously strive to enhance competitiveness of our customers with a range of value-added products and provide world class support to the Institutions at large by adopting a process approach to excellence.

This shall be enabled by implementing an Information & Privacy Security Management System (IPSMS), with the involvement of relevant stakeholders for:

- Ensuring enhanced customer experience & meeting applicable requirements
- Proactively protecting & ensuring security & privacy of PII (Personally Identifiable Information) data and information assets
- Fulfilling compliance obligations to applicable country specific privacy laws and regulations
- Ensuring information security & privacy through design, risk management, change management & applicable controls.
- Cascading information security and privacy requirements to Suppliers thereby ensuring the customer value chain is compliant.
- Continually improving the information management system and processes.

This policy and supporting policies, are part of the IPSMS, are to be adhered to by all entities included in the QSIP scope.

The confidentiality, integrity, availability, and privacy of information, in all its forms, are critical to the ongoing functioning and good governance of QSIP. Failure to secure information increases the risk of financial and reputational losses from which it may be difficult for QSIP to recover. This information & privacy security policy outlines the QSIP approach to information & privacy security management. It provides the guiding principles and responsibilities necessary to safeguard the security & privacy of the QSIP information systems. Supporting policies, codes of practice, procedures, and guidelines as documented in QSIP's Information & Privacy Security Management System (IPSMS), provide further details.

QSIP is committed to a robust implementation of Information & Privacy Security Management. It aims to ensure the appropriate confidentiality, integrity, availability of data

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

and protection of privacy as potentially affected by the processing of PII (Personally Identifiable Information). The principles defined in this policy will be applied to all the physical and electronic information assets for which the QSIP is responsible. QSIP is specifically committed to protection of privacy while processing PII (Personally Identifiable Information), preserving the confidentiality, integrity, and availability of documentation and data supplied by, generated by, and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security and privacy standard ISO 27001 & ISO 27701 and applicable country specific legal/regulatory compliance requirements, specifically GDPR (EU 2016/679).

4 Revisions

Revisions to this document will be made annually, or whenever deemed necessary.

5 Scope

This policy applies to all locations of QS working for QSIP, employees of the parent company, and correspondingly freelance individuals working for QSIP (referred to as "Employees "). It also applies to information received from Clients (referred to as "Controllers"), external service providers and/or guests (referred to as "Sub-processors" or "External parties "), to whom non-disclosed information is communicated or made available by QSIP. This document will be revised annually or when significant changes occur. No employee & contractors are exempt from this policy.

6 Purpose

The purpose of this policy is to protect the QSIP information assets from all threats, whether internal or external, deliberate, or accidental.

The structural elements of this policy:

- Policy context and the objectives defined by senior management.
- System governance and organization for information & privacy security of QSIP
- Developed principals and security & privacy rules conform to the best practices of information & privacy security and are applicable within the entire QSIP.

7 Information & Privacy Security Policy

The Information & privacy Security Policy statement as provided in Section 1 above applies to QSIP including its subsidiaries mentioned in the scope. Information & privacy security policy are required to be understood and underlying QSIP IPSMS implemented for all

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

employees, sub-processors, suppliers, contractors, sub-contractors, and users of the QSIP's information system, regardless of their activities.

This policy may be supplemented with additional specific policies in relation to commercial offers when appropriate. Supplementary policies and measures define the specific security and privacy arrangements put in place to complement the principles and security & privacy regulations specified in the policies. Country Specific data protection requirements including GDPR requirements e.g., Data Processing Agreements (Art.28), Technical and Organization Measures (Art.28 & 32), Inventory of data processing (including protection of privacy as potentially affected by the processing of PII (Personally Identifiable Information)) and Data Flow Diagrams), Transfer Impact Assessment (Art.46 Chapter V), EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Data Protection Impact Assessment (Art.35), Records of processing activities (Art. 30) etc. shall be ensured through IPSMS procedures and controls, as per the Statement of Applicability.

8 Policies Review

At a minimum, the information & privacy security policy is reviewed yearly or after significant changes related to

- Organizational, legal, regulatory, contractual and/or technological contexts
- Security & privacy best practices
- Threats and vulnerabilities
- Discussions on IPSMS risk assessments
- Changes to IPSMS
- Improvements resulting from periodic reviews and audits.

9 Approval

The IPSMS policies have been developed by business, process owners and reviewed by CISO and have been formally approved by the respective policy owners/senior management. The policies are communicated to all users that are likely to interact with the QSIP information system and Its application is mandatory.

10 QSIP organisation

10.1 Senior Management

Strategic decisions and matters regarding the privacy and security requirements for the information system are managed by senior management. Our Senior management demonstrates leadership and commitment concerning information & privacy security by:

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

- Ensuring the information & privacy security policy and the information & privacy security objectives are established and are compatible with the strategic direction of QSIP.
- Ensuring the integration of the information & privacy security management system requirements into the organization's processes.
- Ensuring that the resources needed for the information & privacy security management system are available.
- Communicating the importance of effective information & privacy security management and of conforming to the information & privacy security management system requirements.
- Ensuring that the information & privacy security management system achieves its intended outcome(s). Directing and supporting persons to contribute to the effectiveness of the information & privacy security management system.
- Promoting continual improvement.
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

10.2 Chief Information Security Officer (CISO)

Senior management appoints a CISO responsible for information systems security and privacy. The CISO plans, coordinates, and monitors all activities related to IS security & privacy. The role of the CISO is as follows:

- Lead and coordinate the actions of the group of users associated with information system security and privacy.
- Assist and advise about risks and security & privacy measures to be implemented during the development of new systems.
- Define and propose means of protection and actions required to achieve security & privacy objectives.
- Ensure that solutions are adapted to the issues of security & privacy and comply with the requirements of the information & privacy security policy.
- Define and consolidate periodic reporting to senior management (Management Review Meeting- MRM)
- Responsible for Information & Privacy Security Management System implementation
- Makes periodical review and updates on IPSMS process to ensure the efficiency and effectiveness of information & privacy security controls.
- Communicating Regular updates on changes to legislation, internal IPSMS process or methods to employees
- Monitoring Information & Privacy Security Incidents and take appropriate actions.
- Evaluating compliance with the company processes through regular Internal Audits
- Organization of information & privacy security trainings for all employees
- Organizing security & privacy awareness campaigns to enhance the security & privacy

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

culture and develop a broad understanding of the IPSMS requirements.
- Ensuring that internal audits are periodically conducted, and action items are taken to closure.
- Appropriate contacts with relevant authorities (regulatory, legal) must be maintained.
- Providing a vision to the organization from security & privacy standpoint.

10.3 Privacy officer

Privacy officer shall Support the Data Protection Officer where required in providing and maintaining the necessary documentation as per ISO 27701, to demonstrate compliance with the GDPR, and other applicable country specific privacy laws. Key responsibilities include:

- Informing and providing expert advice to all members of staff in his/her respective country of responsibility regarding their obligation to comply with the provisions of the GDPR and relevant country specific local laws and regulations when processing personal data.
- Monitoring compliance with the Data Protection Policy and any other internal documents relating to data protection in his/her respective country of responsibility and informing the Data Protection Officer of any non-compliance in a timely manner.
- Act as the main point of contact for employees in his/her respective country of responsibility and will cooperate with all members of staff on matters of data protection.
- Takes the necessary steps in his/her respective country of responsibility to execute and roll-out Data Breach Response and Notification Procedure which specifies the process and procedures for reporting personal data breaches and takes the necessary measures to inform the Data Protection Officer accordingly.
- Ensures that training and awareness is available and delivered to all members of staff involved in the processing of personal data in his/her respective country of responsibility.

The following responsibilities can be considered, in consultation Data Protection Officer, if they do not conflict with the key activities listed above:
- Review/develop procedures and other controls for the protection of personal data.
- Establish adequate controls to ensure and maintain the confidentiality, integrity, and availability of personal data.
- Contribute to the business continuity and disaster recovery planning process to ensure that personal data processing is considered.
- This role shall report to Data Protection Officer (DPO)

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

10.4 Line Managers

Managers are responsible for the administration and review of access and authorization of users to their services. With the assistance of CISO, assure that their teams are aware of information system guidelines and security & privacy policies.

10.5 Data Protection Officer (DPO)

The Data Protection Officer assures that all necessary measures have been taken by the QSIP Group about legal, regulatory, and contractual issues. Regarding information system security and privacy, the mission of the DPO is to:

- Keep up to date with judicial standards and jurisprudence, in collaboration with the CISO to communicate and state internal obligations related to information system security & privacy.
- Monitors compliance with GDPR, with other Union or Member State data protection provisions, with other applicable country specific data protection regulation and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- Ensure compliance with legal, regulatory, and contractual provisions concerning information system security & privacy.
- In collaboration with the CISO & privacy officer, identify and maintain legal, regulatory, and contractual obligations.
- Document and update the procedures used to meet legal, regulatory, and contractual obligations.
- Ensure, in collaboration with personnel concerned, the integration of security & privacy requirements in contracts with all service providers or external partners.
- Proceed with regular review of contracts.
- Establish legal references.
- Cooperates with the supervisory authority.
- Contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, about any other matter
- The DPO plays a supporting role to the various entities. Therefore, the DPO may be consulted when or if further information is required.
- Ensures to have due regard to the risk associated with processing operations, considering the nature, scope, context, and purposes of processing.

QS QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

10.6 Human Resource

Human resource management shall apply the security & privacy rules during the processes of the arrival and departure of employees according to ISO 27001 control A 7. Human resource management and ISO 27701 6.4. "People controls", controls the disciplinary processes related to non-compliance with the QSIP Group's practices and security & privacy measures.

10.7 Users

Users must comply with all security & privacy rules which are communicated to them and report, as quickly as possible, any security and privacy incidents, to their Line manager and CISO for further actions.

11 Operations

11.1 Change Management

We aim to prevent malfunctioning of the information system as part of the implementation of changes on platforms (application and system updates, changes in infrastructure, architecture) while maintaining the responsiveness of teams. Security and privacy are an integral part of the entire project lifecycle. Risk Management process is invoked to support the change management process.

11.2 Management of Technical vulnerabilities

As per a risk-based approach, technical vulnerabilities are evaluated and updated regularly to guard against attacks by correcting known vulnerabilities in systems and applications. Vulnerability Management comprises of planning, implementation and operation of Vulnerability Management, Patch Management, Threat Intelligence, Configuration Management, Monitoring Activities and Web Filtering complying with adequate regulations. Periodic internal and third party (external) penetration testing is conducted to assess and analyse the risk of any new vulnerabilities.

External penetration testing covers:

- Web Application Security Assessment
- Web Service Security Assessment
- Security Configuration Review

11.3 Antivirus Protection

QS safeguards its information system against viruses, malicious code attack, Cyber-attack protecting vulnerable systems from these threats, as well as information system input and output.

QS QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

The QS staff systems are equipped with antivirus software, the software provider updates the antivirus databases periodically after reviewed with QS corporate IT. Configuration of the antivirus software is managed by the QS corporate IT support -helpdesk. Users cannot change the configuration or uninstall the antivirus.

11.4 Backups

In the event of incidents affecting the availability or integrity of assets, we ensure to protect against data loss. Safeguard mechanisms are in place for all systems and data including backups (Application configuration, Application source code, Application logs, Access logs, Database logs, configuration files, code, product databases supporting Client data). Business continuity plans are in place and regularly evaluated.

11.5 Monitoring and Logging

All critical functions and systems are monitored by Infrastructure support along with data traceability. The Visualizing tool is used to manage log reports and is reviewed regularly. All the systems and equipment are synchronized to a unique time source. Logs are analysed by the Infrastructure Head based on abnormality and the legal retention period of logs is consistent with the law. The log reports are stored in protected areas.

11.6 Disposal

All computer equipment containing business information is discarded using a secure erasure process. Paper documents containing sensitive and/ or confidential information are destructed using a Paper shredder as per our information & privacy security Policy. Procedures are established for secure disposal of information security assets. A data retention policy is established for normal working. In case of client data, applicable contractual and legal/regulatory requirements are ensured.

12 Compliance to legal, regulatory, and contractual obligations

We respect legal, regulatory, contractual, requirements and adopt applicable standards.

The key drivers and mechanism include the following:

- Local legal and regulatory compliance requirements (E.g., for GDPR, these include related data processing agreements and standard contractual clauses as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021 and related EDPB guidelines).
- Obligations under standard contracts or conditions of service offerings with suppliers/Sub Processors

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

- Obtaining and maintaining certifications recognized for information security management system ISO/IEC 27001, privacy information management system ISO/IEC 27701, Cyber risk, etc.

Compliance is ensured through:

- Up to date legal, contractual, and regulatory requirements and measures as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021 and related EDPB guidelines.
- Observation of any developments in the legal, regulatory, contractual, and standards framework.
- Procedures and their implementation to satisfy legal, regulatory, contractual and standards, Communication channels in place concerning the developments of the framework.
- Monitoring mechanisms can include audit indicators, penetration testing, and vulnerability tests, updates to these tests, and scheduled or annual reviews.
- Action plan for identified non-conformities during audits.

13 Security & Privacy practices

QSIP adopts the best security & privacy practices by defining security & privacy controls applicable to the entire information system of QS Group. Additional security and privacy measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Statement of applicability -is established for the applicable controls required for the context of various products like MoveON and MoveIN that enable Software as a Service (SaaS) offerings. Security & privacy controls and best practices -are to be considered and implemented as appropriate to the risk level.

14 Dealing with Personal data

We have the important responsibility of protecting the personal and sensitive personal data of our clients or prospects by respecting their rights.
Below are the steps ensured at QSIP to protect personal data:

- ISO 27001 and ISO 27701 Controls adopted and implemented as per the Statement of Applicability (refer to Annex B for PIMS-specific reference control objectives and controls (PII Processors))
- Technical and Organisational Measures as required by GDPR and as per European Council, & Commission decision C (2021) 3972 final dated 4.6.2021 (refer Annex A)

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

- Strong Firewall and Anti-virus: Using multiple layers of security software thus making unauthorized access to client data more difficult.
- Access control: Purpose based access provision as per a strong password policy, which ensures changing of passwords to key software systems and immediate access revocation in cases when an employee exit.
- Processing information ethically: Being transparent about data collection and usage and adhering to information handling policies.
- Regular compliance checks against applicable country specific regulations like GDPR
- Data management: Adding value by collecting and managing client data responsibly and strategically, as per contractual and legal/regulatory obligations.
- Supplier management: Ensuring suppliers / sub processors fulfil information security and privacy (including protection of privacy as potentially affected by the processing of PII (Personally Identifiable Information)) through implementation of applicable controls, ensuring the customer value chain is compliant.
- Training and Education: Training stakeholders on ISMS, PIMS, GDPR and Cyber security to enhance the focus on how to manage personal data and maintain confidentiality & privacy.

PIMS-specific reference control objectives and control (PII Processors) steps (refer Annex B) are ensured at QSIP, through the Data Processing Agreement (DPA) and Standard Contractual Clauses (SCC), to protect personal data in cases of cross border transfer.

15 Dealing with Intellectual Property

We respect Intellectual Property when using software subject to license. The licensed software concerning the information system used within QSIP is defined and maintained as part of our Information asset inventory.

The licensing agreements are maintained under the responsible license owner. Requests for installing license software are managed through the proper approval workflow. Regular checks are conducted on the information system to ensure consistency between licensing agreements and current installations.

16 Compliance

Compliance Checks and Internal External Audits are established to verify legal compliance and IPSMS process conformance. Sub-processors and or/any person, who fails to comply with the QSIP IPSMS and legal compliance requirements, shall be subject to appropriate disciplinary and/or legal action.

QS QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

Annex A: Measures based on suggestions from Commission Implementing Decision (EU) 2021/914 dated 4.6.2021.

#	Measures	QSIP Measures
1	Measures of pseudonymisation and encryption of personal data	Personal data is accessible only through secure login and critical data fields are encrypted. All services provided as part of SaaS are accessible only through TLS encrypted communication (or SSH for special packages). The certificates used are checked as part of server maintenance. Hashed passwords for are used for authentication.
2	Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	ISMS based on ISO 27001 is established and implemented, with procedures & controls to ensure identification, authentication, authorization, and accountability. Regular risk management reviews with C, I & A analysis, are conducted to ensure current controls to address the changing threats & vulnerabilities and product releases. Access to systems is restricted and no access is granted to guest or anonymous accounts. For data access, differentiated access rights based on profiles and roles are defined, using the least privilege principle. All data is transferred via secure networks only, with firewalls and anti-virus installed. Appropriate Encryption/tunnelling (VPN) and IP based controls for remote access is implemented. Use of portable data storage media are prohibited. Regular data backups are taken, and backups are stored at two locations, VM Backups are established, with periodic server hardening and OS patching. Power backup is available in case any power failure. Periodic maintenance for the systems/equipment is implemented. Availability is monitored continuously and assured at 99 %. Business continuity plan for processes and services are implemented and tested frequently.

#	Measures	QSIP Measures
3	Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Technical & Organizational Measures (TOM) are in place as per Art. 28 of GDPR. Enough redundancy is built for availability of Class 3 application/ server/ software so that if the primary equipment fails, alternate resource can take over operational activities. physical location of project server is planned so that the server is easily accessible from alternate site during disaster scenario The backup data of critical project server is accessible from alternate location, if required, the recovery of data on to another server is possible in the event of a physical or technical incident. The installable versions of software required is also made accessible in such situations.
4	Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	QSIP is Currently ISO 27001 certified, the requirements for the certification are verified during regular audits. As part of ISMS review, periodic review of TOM with respective data Sub-processors, and thereby compliance to applicable regulations and any changes are checked.
5	Measures for user identification and authorisation	Procedures are documented for identification, authentication, authorization, and accountability of information systems. Access to systems is restricted and no access is given to guest or anonymous accounts. For Data Access, differentiated access rights based on profiles and roles are defined according to business requirement and least privilege concept.
6	Measures for the protection of data during transmission	The data is transferred only over HTTPS to the datacentre we have hosted the application with. QSIP has enabled encryption for HTTPS traffic. Once the data enters to the data centre internal network it is protected with Firewall and IPS protocol. The selected custom fields in the database are stored encrypted by our product. The backups are created with read-only permission and kept in secured backup server. SAML based SSO is implemented, and API access is via secured certificate/key
7	Measures for the protection of data during storage	Data is securely hosted at dedicated data centres. Once data enters the data centre internal network it is protected with Firewall and IPS protocol. Authentication, encryption, and passwords policies are defined and implemented. The selected custom fields in the database are stored encrypted. The backups are created with read-only permission and kept in secured backup server. The internal team conducts regular checks of the application logs.

#	Measures	QSIP Measures
8	Measures for ensuring physical security of locations at which personal data are processed	Technical and Organizational Measures audit being conducted with Data centres on regular intervals and need basis. Regular fire drills are conducted, and equipment is under preventive maintenance. From infrastructure points we have Firewall, IDS and DDOS protection and layered networks. Datacentres have the following measures in place: • Access control policy in place • ISO/IEC 27001, ISO/IEC 27017 and DSS compliance certified • Anti-DDoS: highly resilient Layer 4-7 DDoS protection built into the network
9	Measures for ensuring events logging	Events logging is done using Industry standard logging tools. Protection of log files against unauthorized access is ensured.
10	Measures for ensuring system configuration, including default configuration	Initial product configuration (default) is provided when Institutions are onboarded, and further configuration changes are managed and done by Institutions. For Infrastructure configuration: VM Backups is in place and periodic Server hardening and OS patching is tested and implemented.
11	Measures for internal IT and IT security governance and management	Structured IT Governance mechanism is implemented and regularly reviewed with top management in the MRM. Process Owners are involved in planning, implementing, and monitoring the ISMS processes. Within the scope of their tasks, all employees are responsible for the secure handling of information especially personal data. Access to IT applications and systems are periodically reviewed. Security and Privacy training is provided to all employees.
12	Measures for certification/assurance of processes and products	QSIP Information Security Management System is certified against ISO 27001. Risk management is ongoing to determine weakness and risks, as well as for learning from incidents/ corrective measures. Audits are regularly carried out by internal and external auditors for regular evaluations of information security practices. The corrective action plans for the audit findings have the responsibilities and deadlines assigned. With support from CISO and top management, the audit findings and other related continuous improvement actions are facilitated to closure and reviewed for effectiveness.
13	Measures for ensuring data minimisation	Mandatory data fields are advised by Institutions, thereby ensuring data minimisation by design. Configuration is possible as per instructions provided by Institutions. Personal data is collected and maintained by Institutions.

#	Measures	QSIP Measures
14	Measures for ensuring data quality	Standard practices in Form design are established, with appropriate validation to ensure data quality at point of collection. Erasmus code guidelines are also used. European Student Identifier is used to identify and validate students at various touchpoints. Communication regarding changes / deletion of data types is promptly reconciled with Institutions. Demo and user validation in some cases are conducted to ensure alignment with client data quality requirements. Login Access to forms is restricted
15	Measures for ensuring limited data retention	Data retention is ensured as per the contractual terms with the Institution. Individual's data retention/erasure/deletion is based on Institutions request. Thus, Institutions can specify retention period for specific records under service agreements, and the same will be implemented.
16	Measures for ensuring accountability	CISO and Data Protection Officer are appointed. Process owners are assigned for the ISMS processes and unique usernames, with multi factor authentication are provided for system users. Contracts with Data Centres, along with DPA and regular TOM audits are established. Security and privacy training is provided to all employees at the time of joining and regular refresher training also provided. Periodic reviews and updates as required by ISMS e.g., access rights to personal data, compliance to applicable regulations and changes to regulations are in place. DPIA is in place and updated regularly. Data inventory and related processing activities are available and regularly reviewed.
17	Measures for allowing data portability and ensuring erasure	As per contractual requirements, support can be provided for data portability and erasure. Data can be exported in a standard readable format, on request of the Institution, thereby ensuring data portability.

Annex B: QSIP PIMS-specific reference control objectives and controls (PII Processors)

Annex B Clause #	Title	Control	QSIP undertakes through the Data Processing Agreement:
B.8.2 Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purpose.			

QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

Annex B Clause #	Title	Control	QSIP undertakes through the Data Processing Agreement:
B.8.2.1	Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in helping with the customer's obligations, (considering the nature of processing and the information available to the organization).	where relevant, QSIP contracts with customers and suppliers to process PII, addresses QSIP's role in helping with the customer's obligations, (considering the nature of processing and the information available to QSIP).
B.8.2.2	Organization's purposes	The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.	to ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
B.8.2.3	Marketing and advertising use	The organization shall not use PII processed under a contract for the purpose of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.	as a processor, does not use PII processed under a contract for the purpose of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. QSIP privacy policy ensures that it shall not make such consent a condition for providing the service
B.8.2.4	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	to inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.
B.8.2.5	Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	to provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.
B.8.2.6	Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the application contract) for the	to determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the contract) for the processing of PII carried out on behalf of a customer.

Annex B Clause #	Title	Control	QSIP undertakes through the Data Processing Agreement:
		processing of PII carried out on behalf of a customer.	
B.8.3 Obligations to PII principals Objectives: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.			
B.8.3.1	Obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.	to provide the customer with the means to comply with its obligations related to PII principals.
B.8.4 Privacy by design and privacy by default Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission, and disposal) are limited to what is necessary for the identified purpose.			
B.8.4.1	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.	along with Technical and Organisational Measures, Acceptable Use of IT Systems policy, and Employee Declaration, to ensures that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
B.8.4.2	Return, transfer, or disposal of PII	The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.	along with Technical and organisational measures and its Privacy Policy, to provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.
B.8.4.3	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to	along with Technical and organisational measures, to subject PII transmitted over a data-transmission network to appropriate controls

QUACQUARELLI SYMONDS
QS Quacquarelli Symonds Ltd: Registered (England and Wales) 02563879
Registered Office: 1 Tranley Mews, Fleet Road, London, NW3 2DG, United Kingdom
Tel: +44 (0)20 7284 7200 Fax: +44 (0)20 7284 7261 Web: qs.com

Annex B Clause #	Title	Control	QSIP undertakes through the Data Processing Agreement:
		ensure that the data reaches its intended destination.	designed to ensure that the data reaches its intended destination.
B.8.5 PII sharing, transfer and disclosure Objectives: To determine whether and document when PII is shares, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.			
B.8.5.1	Basis for PII transfer between jurisdictions	The organization shall inform the customer in a timely manner of the basis for PII transfer between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.	to inform the customer in a timely manner of the basis for PII transfer between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract. Inventory of data processing (including protection of privacy as potentially affected by the processing of PII (Personally Identifiable Information)) and Data Flow Diagrams, where applicable, shall be maintained. Transfer Impact Analysis (TIA) is undertaken only in cases where cross border transfers of personal data of EU data subjects outside Europe is involved as applicable under the purview of GDPR.
B.8.5.2	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can be transferred.	to list, specify and document the countries and international organizations to which PII can be transferred
B.8.5.3	Records of PII disclosure to third parties	The organizations shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	to record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.
B.8.5.4	Notification of PII disclosures requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.	to notify the customer (refer QSU_Communication_Matrix) of any legally binding requests for disclosure of PII.

Annex B Clause #	Title	Control	QSIP undertakes through the Data Processing Agreement:
B.8.5.5	Legally binding PII disclosures	The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures that are authorized by the corresponding customer.	to reject any requests for PII disclosures that are not legally binding, consult the corresponding customer (refer QSU_Communication_Matrix for Procedure for dealing with investigation requests from government agencies) before making any PII disclosures that are authorized by the corresponding customer.
B.8.5.6	Disclosure of sub-contractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.	to disclose any use of subcontractors to process PII to the customer before use.
B.8.5.7	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.	to only engage a subcontractor to process PII according to the customer contract.
B.8.5.8	Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.	that, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

End of the document.