Technical and Organizational Security Measures for Questionmark

Last Updated – December 19, 2023

Definitions and what this document covers

This document outlines the high-level overview of the technical and organizational security measures implemented within the Questionmark commercial Software as Service (SaaS) solutions. More details are available publicly at https://www.questionmark.com/trust-center/ ("Trust Center") and privately in our Comprehensive Security Pack, available upon request following execution of a non-disclosure agreement.

This document covers the measures in place for the core Questionmark SaaS solutions provided by Learnosity which are hosted in US (United States), European (UK), Central European and Australian data centers. For some optional parts of the services offered to Customers, including proctoring and badging, Learnosity uses third party subprocessors. For such optional parts of the services, Learnosity has written contracts in place that provide for implementation of adequate security measures which may vary from the below measures for Learnosity delivered services. The document also does not describe our FedRAMP authorized service Questionmark Government.

Within this document, the following definitions apply (and any capitalized terms used without definitions have the definitions given to those terms in the Questionmark Standard terms and conditions at http://www.questionmark.com/go/agree-od-tc):

- "Company" or "We/we" means Learnosity, encompassing six distinct legal entities Questionmark Corporation, Questionmark Computing Limited, Questionmark GmbH, Learnosity Limited, Learnosity Inc and Learnosity Pty Limited.
- "Customer" means any purchaser of Questionmark.
- "Questionmark" means the commercial SaaS provided to the Customer for the creation, delivery, monitoring and reporting of Assessments.
- "Personal Data" means any information provided or submitted by the Customer or Participants in the creation, participation or reporting of Assessments and the output of the Assessments, in each case relating to any identified or identifiable natural person, that Company processes on behalf of Customer.
- "Personnel" means Company employees and authorized individual contractors.

- "Strong Encryption" means the use of industry standard encryption measures compliant with FIPS 140-2.

We may change these measures from time to time. This may mean that security measures are reorganized and/or individual measures are replaced by new measures that serve the same purpose or deal with the same risks without materially diminishing the security level. You can check the latest version of this document at www.questionmark.com/go/od-measures. In the unlikely event that we materially reduce these security measures, we would formally notify Customers.

1. Organization of Information Security

Objective

Company has an information security function that has been ratified and is supported by business leadership and we ensure that our Personnel are competent in information security.

Measures include:

a) We employ Personnel with full-time responsibility for information security.

b) We have a cross-departmental Security Advisory Board to address information security across different areas of business.

c) The information security function reports to a senior board-level executive.

d) We have a comprehensive set of information security policies, approved by senior management and disseminated to all Personnel.

e) Security policies are reviewed at least annually and updated when needed.

f) All Personnel have signed legally reviewed confidentiality agreements that apply during and post-engagement. All Personnel must sign and annually agree to follow rules of behavior that are designed to ensure Personnel understands and follows the Company's information security rules.

g) Failure of Personnel to follow information security policies may be treated as a disciplinary matter and lead to sanctions, including dismissal.

h) All Personnel are given regular training in information security (in the form of videos, presentations, newsletters, emails, etc.) and must take and pass a test on information security as part of their onboarding and thereafter annually. In addition to this, all Personnel are also given data privacy training as part of their onboarding and

annually. Personnel in specialist technical functions take part in role-based security training relevant to their position.

i) Information security is a basic design and architectural principle for Questionmark.

j) We are committed to continual improvement of security.

2. Information Security Management System

Objective

Company has an Information Security Management System ("ISMS") in place to evaluate risks to the security of Customer and Personal Data, to manage the assessment and treatment of these risks and to continually improve its information security.

Measures are:

a) Company has deployed an ISMS to manage security professionally and Company and its ISMS has been and continues to be audited by an independent, external auditor and certified under ISO/IEC 27001:2013 (or a later version of ISO 27001).

b) ISO/IEC 27001:2013 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS, including the assessment and treatment of information security risks. A copy of our ISO 27001 certificate and other information on our security certifications is available online at our Trust Center.

3. Physical Access

Objective

Physical access to Personal Data is protected.

Measures include:

a) Company runs the Questionmark commercial SaaS solutions from ISO 27001 certified and SOC 2 accredited, professional, third party production data centers with defined and protected physical perimeters, strong physical controls including access control mechanisms, controlled delivery and loading areas, surveillance and 24x7x365 guards. Only authorized representatives have access to the data center premises.

b) Power and telecommunications cabling carrying Personal Data or supporting information services at the production data center are protected from interception, interference and damage.

c) Production data centers and their equipment are physically protected against natural disasters, malicious attacks and accidents.

d) Equipment at the production data centers is protected from power failures and other disruptions caused by failures in supporting utilities, and is correctly maintained.

e) Equipment or disk media containing Personal Data (including faulty or end of life disks) are not physically removed from the production data center unless securely erased prior to such removal or being transferred securely for destruction at a third-party site.

f) When Personal Data is copied electronically by Company outside the production data center or between production data centers, appropriate physical security is maintained and the data is subject to Strong Encryption at all times.

4. System Access

Objective

Company data processing systems are used only by approved, authenticated users.

Measures include:

a) Access to Company internal systems is granted only to Personnel and/or to permitted employees of Company's subcontractors and access is strictly limited as required for those persons to fulfill their function.

b) All users access all Company systems related to Questionmark with a unique identifier (user ID).

c) Company has established a password policy that prohibits the unauthorized sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfill defined minimum requirements and are stored in encrypted form. Each computer has a password-protected screensaver.

d) Multi-factor authentication is required for access to online systems containing Personal Data.

e) Company has a thorough procedure to deactivate users and their access when a user leaves the company or to alter their access rights if their job function has changed.

f) Company uses appropriate firewall technology consistent with good industry practice that are designed to protect web applications/servers and virtual machines from web-based attacks at the production data center.

g) For Customer access to Questionmark: initially, we provide the Customer with master credentials for a single root administrator account; then each Customer is responsible for creating, managing and deleting their own administrators and participants. Questionmark provides a wide range of authentication capabilities, including the ability for Customers to set their own password policies and support for SAML 2.0.

5. Data Access

Objective

Persons entitled to use data processing systems gain access only to the Personal Data that they are authorized to access.

Measures include:

a) Company restricts Personnel access to files and programs on a "need-to-know" basis.

b) Company has a formal background check procedure and carries out background checks on all new Personnel with access to Personal Data in accordance with the requirements of applicable laws.

c) Personnel training covers access rights to and general guidelines on definition and use of Personal Data.

d) Where appropriate and practical, we employ data minimization and pseudonymization to reduce the likelihood of inappropriate access to Personal Data.

e) The production environment for Questionmark is separate from the development and testing environment, and application software development Personnel do not have access to Questionmark production environment.

f) We use up-to-date anti-malware software on all appropriate computers and servers.

g) We use well-configured firewalls for Questionmark.

h) Questionmark contains versatile capabilities to set roles and permissions to let Customers manage authorizations to ensure that Personal Data is only made available to appropriate users when needed.

i) We ensure that appropriate Personnel receive alerts and notifications from system software vendors and other sources of security advisories and install system software patches regularly and efficiently.

6. Data Transmission

Objective

Prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during transfer.

Measures include:

a) Customer access to Questionmark is protected by TLS 1.2 or higher.

b) We configure TLS for security, for an up-to-date report on the configuration of our main systems, see:

- Questionmark US - https://www.ssllabs.com/ssldb/analyze.html?d=ondemand.questionmark.com
- Questionmark EU - https://www.ssllabs.com/ssltest/analyze.html?d=ondemand.questionmark.eu
- Questionmark AU - https://www.ssllabs.com/ssltest/analyze.html?d=ondemand.questionmark.au
- Questionmark EU Central - https://www.ssllabs.com/ssltest/analyze.html?d=eucentral.questionmark.com

c) We use Strong Encryption for all other transmission of Personal Data outside the production data center.

d) Any Personal Data stored outside the production data centers are protected by Strong Encryption at rest.

The Customer is responsible for the security of Personal Data once it has been transmitted from Questionmark to the Customer, including when downloaded or accessed by Customer users.

7. Development Process

Objective

Company implements administrative and technical controls to ensure secure code development.

Measures include:

a) Company has a defense in depth approach to product development and uses a Secure Development Lifecycle (SDLC) that includes a wide range of security testing and flaw reporting and management procedures.

b) Company trains its software engineers and quality assurance Personnel on its Product Development Security Policy, which includes application security practices and secure coding practices.

c) Company has one or more secured repositories of product source code, which is accessible only to authorized Personnel.

d) Security testing includes code review and appropriate security analysis on a periodic basis to identify flaws.

e) All changes to software on Questionmark are via a controlled, approved release mechanism within a formal change control program that tracks, documents, tests, and approves change requests prior to implementation.

f) All encryption and other cryptographic functionality used within Questionmark (except for interfaces to third parties) that has a security purpose uses industry standard encryption and cryptographic measures aligned with the standards promulgated with FIPS 140-2.

8. Availability

Objective

Personal Data is protected from accidental destruction or loss, and there is timely access, restoration or availability to Personal Data in the event of an incident.

Measures include:

a) We use N+1 redundancy at the production data center so that an availability failure of a single system or component is unlikely to impact general availability.

b) The production data center has N+1 power supplies, generators on-site and with battery back-up to safeguard power availability to the data center.

c) The production data center has N+1 internet suppliers to safeguard connectivity.

d) The production data center is monitored 24x7x365 for power, network, environmental and technical issues.

e) We create frequent, encrypted back-up copies of Personal Data and these are stored in a geographically separate location to the data center. Appropriate measures to flag backup failures and to conduct regular restore tests are in place.

f) We have a Business Continuity Plan in place which is regularly reviewed and updated.

g) We test elements of the Business Continuity Plan regularly, which concludes with "Lessons Learned" for process improvement.

Current availability of Questionmark can be seen at http://status.questionmark.com. More information on availability measures and a summary of our service continuity plan are available in our Comprehensive Security Pack.

9. Job Control

Objective

Personal Data processed on a Customer's behalf is processed solely in accordance with the relevant agreement between the Customer and Company and related instructions of the Customer, including in the use of subprocessors.

Measures include:

a) Company acts as data processor with respect to Personal Data and stores and processes Personal Data in order to operate Questionmark under the instructions of Customer.

b) Company does not access Personal Data, except to provide services to the Customer which we are obligated to perform in support of the Customer experience, including for general operation and monitoring of Questionmark, troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by Customer.

c) Company uses a limited number of subprocessors to help provide the Questionmark solution, a list can be found at www.questionmark.com/go/od-subprocessors.

d) Company has in place contracts with all subprocessors that provide for confidentiality of Personal Data and agreements incorporating the EU Standard Contractual Clauses (Processors) with all subprocessors that process relevant Personal Data outside of the European Economic Area.

e) Questionmark Corporation, a Learnosity company, is certified to the EU-U.S. Privacy Framework (EU-U.S. DPF), including the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

f) Customers who are purchasing Questionmark EU or Questionmark EU Central solutions are able to contract with either Questionmark Computing Limited in the UK or Questionmark GmbH in Germany. As both of these entities are outside of the US, do not have a US parent company and provide services primarily from third party data centers in UK/EU, they are unlikely to receive a data access request from US law enforcement.

g) After termination of the agreement with Customer, Company works with the Customer to check that the Customer has recovered the Personal Data that it needs from Questionmark, and once this is confirmed, initiates a deletion process for Personal Data and other data stored in the Questionmark solution. Deletion can happen more quickly on request, but ordinarily Personal Data stored in Questionmark is deleted within a total timeframe of 3 months, to allow for time for such data to cycle out of backup and in case Customers later realize that they need further data. Limited Personal Data may be retained for a further three months for technical reasons but is then deleted.

10. Data Separation

Objective

Personal Data from one Customer is always logically or physically separated from that of other Customers.

Measures include:

a) Company architects its systems to ensure logical or physical separation of Personal Data originating from different Customers.

b) In each step of the processing, Personal Data received from different Customers can be identified so data is always physically or logically separated.

c) Any audit rights given to Customers to review Company systems and security always respect the rights of other Customers. including preventing access to data from other Customers.

11. Incident Management

Objective

In the event of any security breach of Personal Data, the effect of the breach is minimized and the Customer is promptly informed.

Measures include:

a) Company maintains an up-to-date Incident Response Plan that includes responsibilities, and how information security events are assessed and classified as incidents.

b) Company has monitoring and logging systems at the production data center to provide records of events on the system.

c) The clocks of all systems at each production data center are synchronized to a single reference time source to aid investigation in the event of an incident.

d) Company regularly tests its Incident Response Plan with "table-top" exercises, along with functional testing.

e) In the event of a Personal Data breach that requires notification according to applicable laws, Company will notify Customers without undue delay after becoming aware of the Personal Data breach to the email address or other contact information specified by Customers for this purpose or to Customers' general contact if no specific breach notification contact information has been provided. In such event, Company shall provide all information on the Personal Data breach to Customers as required by applicable laws (including where applicable the EU General Data Protection Regulation ("GDPR") or UK GDPR), which information may be provided incrementally if not immediately apparent (but in any case without undue delay) and will include where required by applicable law our explanation of the possible consequences the Personal Data breach. Company shall take reasonable, necessary measures to mitigate the effects of the Personal Data breach.

12. Compliance

Objective

Company commissions third party audits to measure the effectiveness of the technical and administrative controls included in these measures against industry standard security frameworks.

Measures include:

a) We conduct regular internal and external audits of our security.

b) We have a formal policy for managing suppliers who have access to Personal Data and this includes criteria for reviewing and approving suppliers and procedures for monitoring and reviewing their performance.

c) We take reasonable steps to ensure that Personnel are aware of and comply with the technical and organizational measures set forth in this document.

d) We conduct regular application vulnerability scans and manual penetration tests on appropriate parts of Questionmark using reputable third party service providers. Further details are available in our Comprehensive Security Pack.

e) We also permit Customers upon written request and prior approval to perform their own penetration tests as long as the testing does not negatively affect the Questionmark solution or other Customers' use of Questionmark.

Appendix 1

Supplementary Measures for Personal Data subject to the GDPR/UK GDPR

Company commits to the following supplementary measures in respect of Personal Data subject to the GDPR or UK GDPR that is transferred to outside of the European Economic Area or United Kingdom pursuant to the Standard Contractual Clauses published by the European Commission under Commission Implementing Decision (EU) 2021/914 (4 June 2021) ("SCCs").

1. Company has never received a valid and binding demand for Personal Data from the U.S. intelligence authorities, including under FISA s.702 or EO 12333 and with respect to EEA or UK Personal Data transferred to the U.S. under the SCCs (or any prior version), and commits to removing or modifying this statement in the event this position ever changes in accordance with applicable laws;

2. Company will enter into the SCCs which in its view implement the obligations of the Schrems II decision of the Court of Justice of the European Union and which warrant that it believes that it is not required to grant access to data to the US intelligence authorities under Section 702 FISA (or EO 12.333). The SCCs contain contractual provisions on notification and handling government data demands in accordance with the expectations of the European Data Protection Board. We believe that law enforcement and national security agencies should go directly to our business and government customers to obtain information or data regarding those entities, their employees, and users.

3. Company will commit to challenge any FISA s.702 or other valid and binding demand that it believes in good faith is unauthorized or overbroad and defend itself against orders to hand over data in court as far as reasonably possible. We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with valid and binding demands when we are clearly compelled to do so. Our first step is always to use every reasonable effort to re-direct such orders to customers or to inform them, to allow customers to seek a protective order or other appropriate remedy. If ever ultimately compelled to do so, we would only disclose the minimum necessary data to satisfy the request;

4. Company will maintain and comply with a government access request policy which has been formally approved by its executive management. In the event of government access, Company will promptly notify impacted customers, unless prohibited under the

law applicable to the requesting third party, and, if prohibited from notifying Customer, use reasonable lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible. Lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction or where in the opinion of legal counsel there is no realistic prospect of success;

5. Company uses end to end encryption of Customer Personal Data in transit and at rest. Note that although such files do not usually contain personal data, encryption at rest may not include video, audio and other files uploaded into Questionmark.

6. Company's information security management system is assessed for compliance with our security and privacy policies, standards, and controls, which are based on ISO 27001 and other internationally recognized industry standards.

7. Company has always had and will continue to have a "no backdoor policy". Our product development practices prohibit any intentionally developed capabilities or product features that are designed to allow undisclosed and/or undocumented device or network access, or undisclosed and/or undocumented access to device information and/or services.

8. Company encourages customers to avoid sending personal data by email for technical support purposes.

9. We confirm that data subjects have rights under the GDPR, including the right to compensation for material or non-material damage under and in accordance with Article 82 GDPR;