Technical and Organizational Security Measures for Questionmark's OnDemand Service

Last Updated – December 6, 2022

This document describes technical and organizational security measures implemented by Questionmark Corporation, Questionmark Computing Limited and Questionmark GmbH, ("Questionmark") to protect Personal Data and ensure the ongoing confidentiality, integrity and availability of Questionmark's commercial OnDemand Service comprising "US OnDemand", "EU OnDemand", "AU OnDemand" and "EU Central OnDemand." This document does not describe our FedRAMP authorized service OnDemand for Government.

This document covers the measures in place for the core Questionmark OnDemand Service. For some optional parts of the services offered to Customers, including proctoring and badging, Questionmark uses third party subprocessors. For such optional parts of the services, Questionmark has written contracts in place that provide for implementation of adequate security measures which may vary from the below measures for Questionmark delivered services.

Questionmark may change these measures from time to time. This may mean that 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 Questionmark does materially reduce its security measures, Questionmark shall formally notify Customers.

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

- "Customer" means any purchaser of the OnDemand Service.
- The "OnDemand Service" means the Software-as-a-Service provided by Questionmark 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 Questionmark processes on behalf of Customer.
- "Personnel" means Questionmark employees and authorized individual contractors.
- "Strong Encryption" means the use of industry standard encryption measures compliant with FIPS 140-2.

This document is a high-level overview of Questionmark's technical and organizational measures. More details on the measures Questionmark implements are in publicly available white papers at

https://www.questionmark.com/resources/whitepapers/ and in Questionmark's Comprehensive Security Pack available upon request following execution of a non-disclosure agreement ("NDA").

1. Organization of Information Security

Objective

Questionmark has an information security function that has been ratified and is supported by business leadership and Questionmark ensures that its Personnel are competent in information security.

Measures include:

a) Questionmark employs Personnel with full-time responsibility for information security.
b) Questionmark has a cross-departmental Security Board to address information security across different areas of business.
c) The Questionmark information security function reports to a senior executive who is on the board of Questionmark's parent company.
d) Questionmark has a comprehensive set of information security policies, approved by senior management and disseminated to all Personnel.
e) Questionmark 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 annually agree and sign user rules of behavior that are designed to ensure Personnel understands and follows Questionmark'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 a 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 led by Questionmark legal team and must complete a data privacy quiz as part of their onboarding and annually. Personnel in Systems Operations, Product Development, Platform, and Security functions take part in role-based security training relevant to their position.
i) Information security is a basic design and architectural principle for the OnDemand Service.
j) Questionmark is committed to continual improvement of its security.

2. Information Security Management System

Objective

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

Measures are:

a) Questionmark has deployed an ISMS to manage security professionally and Questionmark and its ISMS has been and continues to be audited by an independent, external auditor and

certified under ISO/IEC 27001:2013. Questionmark's formal certification covers Questionmark Computing Limited, Questionmark Corporation and Questionmark GmbH.

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 Questionmark's ISO 27001 certificate and other information on our security certifications is available at Questionmark's Trust Center at https://www.questionmark.com/trust.

3. Physical Access

Objective
Physical access to Personal Data is protected.

Measures include:

a) Questionmark runs the OnDemand Service 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) The production data center and its equipment is physically protected against natural disasters, malicious attacks and accidents.
d) Equipment at the production data center 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 Questionmark outside the production data center, appropriate physical security is maintained and the data is subject to Strong Encryption at all times.

4. System Access

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

Measures include:

a) Access to Questionmark internal systems is granted only to Personnel and/or to permitted employees of Questionmark's subcontractors and access is strictly limited as required for those persons to fulfil their function.
b) All users access Questionmark systems with a unique identifier (user ID).
c) Questionmark has established a password policy that prohibits the sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be

altered. All passwords must fulfil 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) Questionmark 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) Questionmark use Network Security Groups (NSGs) and run Web Application Firewalls (WAFs) on the application gateways that are designed to protect web applications/servers from web-based attacks (HTTP/HTTPS) at the production data center. We run host-based firewalls on the Virtual Machines. For Customer access to the system: initially, Questionmark provides master credentials for a single root administrator account for the Customer; then each Customer is responsible for creating, managing and deleting their own administrators and participants. Questionmark provides a wide range of authentication capability 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) Questionmark restricts Personnel access to files and programs on a "need-to-know" basis.
b) Questionmark 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, Questionmark employs data minimization and pseudonymization to reduce the likelihood of inappropriate access to Personal Data.
e) The production environment for the OnDemand Service is separate from the development and testing environment, and development Personnel do not have access to the production environment.
f) Questionmark uses up-to-date anti-malware software on all appropriate computers and servers.
g) Questionmark uses well-configured firewalls for the OnDemand Service.
h) The OnDemand Service contains versatile capabilities to set roles and permissions to let Customers manage authorizations to set that Personal Data is only made available to appropriate users when needed.
i) Questionmark ensures that appropriate Personnel receive alerts and notifications from system software vendors and other sources of security advisories and installs 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 the OnDemand Service is protected by TLS 1.2 or higher.
b) Questionmark configures TLS for security, for an up-to-date report on our configuration, see:
    - US OnDemand - https://www.ssllabs.com/ssldb/analyze.html?d=ondemand.questionmark.com
    - EU OnDemand - https://www.ssllabs.com/ssltest/analyze.html?d=ondemand.questionmark.eu
    - AU OnDemand - https://www.ssllabs.com/ssltest/analyze.html?d=ondemand.questionmark.au
    - EU Central OnDemand - https://www.ssllabs.com/ssltest/analyze.html?d=eucentral.questionmark.com
c) Questionmark uses Strong Encryption for all other transmission of Personal Data outside the production data center.
d) Any Personal Data stored outside the production data center is 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
Questionmark implements administrative and technical controls to ensure secure code development.

Measures include:

a) Questionmark 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) Questionmark trains its software engineers and quality assurance Personnel on Questionmark's Product Development Security Policy which includes application security practices and secure coding practices.
c) Questionmark has a central, secured repository of product source code, which is accessible only to authorized Personnel.
d) Security testing includes code review and employing static code analysis tools on a periodic basis to identify flaws.
e) All changes to software on the OnDemand Service 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 the OnDemand Service (except for interfaces to third parties) that has a security purpose uses industry standard encryption and cryptographic measures compliant 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) Questionmark uses 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) Questionmark creates frequent, encrypted back-up copies of Personal Data and these are stored in a geographically separate location to the data center.
f) Questionmark has a system in place to ensure that any failures of backup to operate correctly are flagged and dealt with.
g) Questionmark performs restore tests from those backups regularly.
h) Questionmark has a business continuity plan in place which is regularly reviewed and updated.
i) Questionmark tests elements of its business continuity plan regularly, which concludes with "Lessons Learned" for process improvement.

Current availability of the OnDemand Service 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 and related instructions of the Customer including in the use of subprocessors.

Measures include:

a) Questionmark acts as data processor with respect to Personal Data and stores and processes Personal Data in order to operate the OnDemand Service under the instructions of Customer.
b) Questionmark does not access Customer Personal Data, except to provide services to the Customer which Questionmark is obligated to perform in support of the Customer experience, including for general operation and monitoring of the OnDemand Service, troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by Customer.
c) Questionmark uses a limited number of subprocessors to help it provide the OnDemand Service including a small number of third party companies and some individual (natural person) subcontractors. A list of individual (natural person)

subcontractors is available on request. Third party companies used as subprocessors can be found at www.questionmark.com/go/od-subprocessors.

d) Questionmark has in place directly or via affiliates contracts with all subprocessors that provide for confidentiality of Personal Data and agreements incorporating the EU Standard Contractual Clauses (Processors) in place with all subprocessors that process relevant Personal Data outside of the European Economic Area.
e) Questionmark Corporation remains certified to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks but doesn't rely on them for international data transfers.
f) Customers who are purchasing European OnDemand or European Central OnDemand services are contracted with either Questionmark Computing Limited in UK or Questionmark GmbH in Germany. As both of these Questionmark entities are outside of the US, and do not have a US parent company, providing services from third party data centers in UK/EU, it is unlikely to receive a data access request by US law enforcement.After termination of the agreement with Customer, Questionmark works with the Customer to check that the Customer has recovered the Personal Data that it needs from the OnDemand Service, and once this is confirmed, initiates a deletion process for Personal Data and other data stored in the OnDemand Service. Deletion can happen more quickly on request, but ordinarily Personal Data stored in the OnDemand Service 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

a) Questionmark architects its system 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 Questionmark 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) Questionmark maintains an up-to-date incident response plan that includes responsibilities, and how information security events are assessed and classified as incidents.
b) Questionmark has a centralized monitoring and logging system at the production data center to provide a record of events on the system.
c) The clocks of all systems at the production data center are synchronized to a single reference time source to aid investigation in the event of an incident.
d) Questionmark 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, Questionmark 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 Customer's general contact if no specific breach notification contact information has been provided. In such event, Questionmark 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), which information may be provide incrementally if not immediately apparent (but in any case without undue delay) and will include where required by applicable law Questionmark's explanation of the consequences the Personal Data breach may entail. Questionmark shall take reasonable, necessary measures to mitigate the effects of the Personal Data breach.

12. Compliance

Objective
Questionmark commissions third party audits to measure the effectiveness of these technical and administrative controls against industry standard security frameworks.

Measures include:
a) Questionmark conducts regular internal and external audits of its security.
b) Questionmark has 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) Questionmark takes reasonable steps to ensure that Personnel are aware of and comply with the technical and organizational measures set forth in this document.
d) Questionmark conducts at least quarterly application vulnerability dynamic scans on the OnDemand service using a reputable third party service provider and also conducts at least annually a manual penetration test on the OnDemand Service using a reputable third party service provider. Such scans and tests are performed on a selection of the different data centers used based on risk. Questionmark does permit Customers upon written request and prior approval to perform their own penetration tests as long as the testing does not negatively affect the OnDemand Service or other Customers' use of the OnDemand Service.

Appendix 1

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

Questionmark 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. Questionmark 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. Questionmark 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. Questionmark believes 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. Questionmark 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, Questionmark would only disclose the minimum necessary data to satisfy the request;

4. Questionmark will maintain and comply with a government access request policy, the most recent version of which that has been formally approved within Questionmark. Questionmark will promptly notify 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. Questionmark uses end to end encryption of customer personal data in transit and at rest;

6. Questionmark'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. Questionmark 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. Where customers order a European hosted service, Questionmark will provide assurance that the production data center used to provide the services at which in-scope personal data is stored at rest will be located in the UK or EU. Questionmark encourages customers to avoid sending personal data by email for technical support purposes;

9. Questionmark confirms 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;