Data Protection Agreement

Instructions for signing this DPA
This Data Processing Agreement ("DPA") is entered into between Q-Pathway Ltd, located at Baile na hAille, Moycullen, Galway, Ireland and the "Customer". Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless Q-Pathway Ltd. has separately agreed to those modifications in writing.

This DPA becomes effective on the date that it has been duly executed by both parties.

To complete this DPA, Customer must: Submit a completed and signed DPA to Q-Pathway by email to support@companionqms.com. If you have any questions about this DPA, please contact support@companionqms.com

By signing below, you represent and warrant that you are an authorised representative with authority to sign this DPA.

CUSTOMER	Q-Pathway Ltd
Title:	Title:
Signature:	Signature:
Printed Name:	Printed Name:
Date Signed:	Date Signed:

Data Processing Agreement Terms and Conditions

"Agreement" means the attached Agreement between Q-Pathway Limited ("Q-Pathway") and the Customer under which Services are provided to the customer.

"Data Controller", "Data Subject", "Data Subject Access Request", "Personal Data", "Personal Data Breach," "Data Processing", "Data Processor", Personally Identifiable Information, "Processing" and "Supervisory Authority" have the same meanings as in the GDPR.

"Customer" or "you" means the customer that is identified on, and is a party to, the Agreement.

"Data Protection Legislation" means GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time.

"GDPR" means the General Data Protection Regulation (*(EU) 2016/679*).

"Services" mean the Q-Pathway services ordered or subscribed to by Customer in an Agreement.

1. Introduction

This "Data Processor Agreement" regulates Q-Pathway's processing of Personal Data on behalf of the Customer and is attached as an addendum to the Agreement in which the parties have agreed the terms of the Services to be provided to the Customer.

2. Data Processing

2.1 Scope and roles

The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Data Controller and Q-Pathway is the Data Processor.

2.2 Compliance with laws

The Data Processor and Data Controller confirm that they shall comply with their obligations under Data Protection Legislation.

3. Instructions for data processing

Q-Pathway will only process personal information, such as name, work title and email address, insofar as it is required for the Services and proper functioning, and invoicing Q-Pathway will not access Customer sites unless requested by you or your authorised representatives. Examples of this would be to facilitate upgrades or for support services. For the avoidance of doubt, this shall only occur where further written authorisation is received.

Q-Pathway will process Personal Data in accordance with Customer's instructions as specified in the Agreement and these terms and conditions. The signing of this Agreement is Customer's authorisation and instruction to Q-Pathway in relation to the processing of Personal Data.

The storage of Personal Data with respect to the Services is not expansive; however, depending on your implementation and request for support this may widen due to the scope of what you have determined for capture in your forms.

3.1 Purpose

Q-Pathway will only process Personal Data on written authorisation from the Data Controller.

Q-Pathway does not process or store any personal data that is not needed to perform the Services requested by the Data Controller. The Personal Data that Q-Pathway processes on behalf of the data controller will be accurate, complete, and kept up-to-date insofar as is possible.

Q-Pathway requires that Data Controllers notify their employees and users (i.e., the data subjects) of the Data Processing carried out by Q-Pathway and will obtain their consent for Q-Pathway to do so. Personal Data will not be disclosed, made available, or otherwise used for purposes other than to perform the Services on behalf of the Data Controller, except where otherwise required by law.

3.2 Q-Pathway Personnel
Q-Pathway only permits access to personal data to its personnel who are authorised administrators with appropriate privileges.

3.3 Shared Responsibility Model
As the Services are deployed using Microsoft Azure infrastructure, CompanionQMS, Microsoft and our Customers shall have a shared responsibility when it comes to the application, the data stored in it and how it is accessed. This means that responsibility is shared across three separate parties, Microsoft Azure provides 'the cloud' infrastructure that the application runs on, Q-Pathway deploys the application securely on Microsoft Azure's infrastructure, and the customer is responsible for ensuring that access is secured per their internal IT policies.

4. Security Measures
Q-Pathway ensures the confidentiality and availability of the Personal Data that it processes, and that appropriate technical and organisational measures are taken to protect such Personal Data.

Q-Pathway stores all data including backups in Microsoft Azure storage in European data centres. For durability at run-time CompanionQMS servers utilise locally redundant storage. All Personal Data is persisted in a database that employs full, differential and transaction log backups (every 10 minutes) to geographically redundant storage. In addition, the entire CompanionQMS infrastructure is backed up daily to geographically redundant storage.

Azure is generally recognised to meet a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. All Azure facilities meet a broad set of compliance standards, to safeguard the confidentiality, integrity, and availability of data, details of which can be found here https://azure.microsoft.com/en-gb/overview/trusted-cloud/

4.1 Technical security measures and access control
In terms of protection of the Personal Data held in the system, privacy by design principles are encapsulated within our strong and rigorous approach to information governance in software design and engineering; including encryption, access control and activity logging as follows.

4.2 Authentication
Users must log in using a CompanionQMS username and password. Passwords are stored and retrieved using Windows hashing algorithms, and all data at rest is encrypted through 256-bit AES encryption. CompanionQMS uses claims-based authentication to authentication. User names and passwords are sent securely to CompanionQMS servers using SSL technology.

4.3 Password Management
Companion QMS enforces strong password requirements (i.e. minimum length, with a mix of alphanumeric characters). You and your users shall be responsible for keeping your password secret. Q-Pathway cannot retrieve your password but can reset your password on specific request.

4.4 Securing data in transit
All information is transmitted securely to CompanionQMS servers over HTTPS using modern protocols.

4.5 Securing data at rest
All data stored at rest is encrypted through 256-bit AES encryption.

4.6 Access
Access control user management and access to the system is performed by CompanionQMS on behalf of its customers.

4.7 Activity logging companion
QMS records the activity relating to records such as creation, updating and deletion. Such information allows for an audit trail to identify who, when and what activity was performed on records in the system.

4.8 Purging
It is possible to remove user records and other data that may contain Personally Identifiable Information (PII) from the system in response to a Data Subject Access Request. This would be performed by CompanionQMS administrators. We do advise customers to consider whether there are legal, regulatory or other legitimate reasons to decline the deletion of PII via user records from the system. The permanent loss of this data could be impactful to the successful operation of CompanionQMS or the organisation itself.

5. Personal data breaches notification
Q-Pathway protects Personal Data through reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure.

Q-Pathway will notify the Data Controller without undue delay after becoming aware of a breach and will assist the data controller in reporting to supervisory authorities and affected EU data subjects any breaches.

Microsoft conducts ongoing monitoring and testing of Azure security measures that protect the Azure SQL Database. These include on-going threat modelling, code review and security testing; penetration testing exercises, and centralised security logging and monitoring.

Customer must immediately notify Q-Pathway of any unauthorised uses of a user's profile or any other breaches of security.

6. Rights of the data subjects
Q-Pathway shall, to the extent legally permitted, promptly notify Customer if Q-Pathway receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure (right to be forgotten), data portability, objection to the processing, or its right not to be subject to an automated individual decision making). Considering, the nature of the processing, Q-Pathway shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Legislation.

Q-Pathway shall upon Customer's request provide commercially reasonable assistance to Customer in responding to such Data Subject Request, to the extent Q-Pathway is legally permitted to do so, and the response to such Data Subject Request is required under applicable Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any reasonable costs that Q-Pathway may incur to provide such assistance.

7. Audit
Upon reasonable request, Q-Pathway will endeavour to provide the Customer with reasonable evidence of compliance with this Agreement.

8. International transfers of personal data
Data is located in servers in the Azure West Europe region and is not transferred outside Europe or the EEA.

9. Sub-processors
The Customer consents to the appointment of third party "Sub-processors" under the terms herein. The Data Processor will keep a list of "Sub-processors" which can be made available to the Customer upon written request.

Sub-processor Agreements. Q-Pathway will: (a) enter into a written agreement in accordance with the requirements of Article 28(4) of the GDPR with any Sub-processor that will process Personal Data; (b) ensure that each such written agreement contains terms that are no less

protective of Personal Data than those contained in this DPA; and (c) be liable to the Data Contoller for the acts and omissions of its Sub-processors to the same extent Q-Pathway would be liable if performing the services of each of those Sub-processors directly under the terms of this DPA.

10. Liability

Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Agreement. To the extent permitted by applicable law Q-Pathway's liability to Customer under this DPA will be limited to the same extent as Q-Pathway liability to Customer under the Agreement. For the avoidance of doubt, the total liability of Q-Pathway and its affiliates for all claims by Customer arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA.

11. Duration

The Data Processor Agreement shall remain in force until the Agreement is terminated.

12. Termination

Following expiration or termination of the Agreement, the Data Processor will delete make available all Personal Data in its possession as provided in the Agreement except to the extent the Data Processor is required by applicable law to retain some or all of the Personal Data (in which case the Data Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to such Personal Data post-termination or expiration of the Agreement.