OneQA ROPA Entry Information

Fluke Health Solutions
6920 Seaway Blvd, Everett, WA 98203 USA | (800) 850-4608

General

This document provides customer with information related to use of personal data in the OneQA system that may assist customer to meet its Records of Processing Activity (ROPA) obligations. The information is largely based on ROPA requirements of the EU and UK. References to relevant GDPR articles are included in the document. Similar requirements can be found in other privacy laws around the world. What we have provided are factual details likely to be most helpful in producing the required ROPA. There will be other details that customer will be required to complete based on information available to it. For example, customer will need to consider processing in any additional information systems OneQA interfaces with in customer's environment, including integrations with third party solutions. Although customer is responsible for assessing and complying with the obligations under applicable law to which it is subject, Fluke Healthcare Services (FHS) stands by to assist customer with any questions it may have arising from customer's particular circumstances.

Purpose of Processing

Record (GDPR Ref)	
Purpose of processing (Art 30 (1)(b))	Personal data is processed by the OneQA system for the purpose of enabling the traceability and accountability of technicians performing tests on medical devices, and for operation of the OneQA system. This allows customers to comply with their regulatory testing and documentation obligations in an efficient way.

Details of Data Collected

This section sets out the individual data items collected and the individuals this data is collected about

Data subjects (Art 30(1)(c))	**Personal data category (Art 30 (1)(c))**	**Personal data elements (N/A – good practice)**
"Tenant Member" recorded in OneQA	Profile information	First and last name Email Phone number Company Tenant Role: Tenant Admin, Application Admin, Author, Approver, User Country Username Password [1]
Technician "User" performing tests on equipment using OneQA platform	Test results data	Date test performed Time test performed First and last name Work order

[1] System also captures Team Size and Zip Code for FHS's use as data controller – see OneQA Privacy Data Sheet

Fluke Health Solutions
6920 Seaway Blvd, Everett, WA 98203 USA | (800) 850-4608

		Service Type Asset Information Test Device Information Test results

Lawful Processing/Special Category Personal Data

This section sets out the lawful basis for processing relied upon and whether special categories of personal data are captured.

Record (GDPR Ref)	
Article 6 lawful basis for processing personal data (Art 13 (1)(c))	[The customer may be subject to legal obligations to service/test medical devices to meet minimum performance and safety standards, and these obligations may include requirements for traceability of the person performing the tests. As such, the customer may determine processing personal data as set out is a valid "legal obligation" and described as such in the General Data Protection Regulation (GDPR): *Article 6(1)(c): Processing shall be lawful only if and to the extent that at least one of the following applies: … (c) processing is necessary for compliance with a legal obligation to which the controller is subject."* In addition, the customer may determine processing personal data as set out is a valid "legitimate interest", as described as such in the GDPR: *Article 6(1)(f) GDPR: Processing shall be lawful only if and to the extent that at least one of the following applies: … (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."*]
Special Category Personal Data (Art 13 (1)(c); Art 30 (1)(c))	N/A
Article 9 lawful basis for processing Special Category Personal Data (Art 13 (1)(c))	N/A

Third Parties

This section sets out third parties personal data is shared with which can include data processors or other third parties which receive the data

Record (GDPR Ref)	
Data Processors (Art 13 (1)(a), Art 13 (1)(e), Art 30 (1)(d))	FHS, see DPA at https://www.flukebiomedical.com/onega-software-service-agreement#onega-data-protection. Amazon Web Services (AWS) (sub-processor) See information about AWS's data privacy

	practices and data processing terms at https://aws.amazon.com/compliance/data-protection/.
Other recipients (Art 13 (1)(a), Art 13 (1)(e), Art 30 (1)(d))	N/A

Data Location and International Transfers

This section sets out where the data is stored, both in terms of where the data sits on relevant systems and where the data is stored geographically. It also sets out any specific transfers of personal data outside of the EEA and the safeguards in place to protect the transfers.

Records (GDPR Ref)	
Data Location (Systems) (N/A - good practice)	PC based application in customer's premises Cloud storage on AWS
Data Location (Geographic) (Art 30 (1)(e))	OneQA data is stored on the AWS cloud on servers in the EU (currently, EU-Central in Frankfurt, Germany).
Location of non-EEA transfers of Personal Data (Art 13 (2)(f), Art 30 (1)(e))	Data is not moved or replicated outside of EU (except for limited reporting of tenant user information for day to day operations).
Safeguards in place to protect Non-EEA Transfers (if applicable) (Art 13 (2)(f), Art 30 (1)(e))	SCCs – see https://www.flukebiomedical.com/oneqa-software-service-agreement#oneqa-data-protection.

Retention and Protection

Record (GDPR Ref)	
Retention Period (Art 30 (1)(f))	**Test data in system** This data is kept for 90 days. The customer should move the data to CMMS, which is intended to be the long term record, during this period. **System user data** **Users other than Tenant Admin** – retention of this data is controlled by the Tenant Admin **Tenant Admin** • While accounts active – indefinite. • Deactivated accounts – no fixed retention period but subject to discretionary periodic deletion.
Details of any technical and organisational measures (Art 30 (1)(g))	The following Secure Product Development (SPD) design considerations have been applied: 1. Penetration Testing using Synopsis tool 2. Metrics – monitoring security metrics e.g. from penetration testing and addressing issues according to priority 3. Static application security testing (SAST) is performed using Veracode 4. Approved Tools – Synopsis and Veracode are approved security tools 5. 3rd Party Risk – AWS is an industry leading cloud supplier 6. Training – AWS training 7. Incident Response – ticketing systems to manage any incidents

	8. Security Requirements – penetration testing, SAST and DAST 9. Design for Security – follow AWS architecture and design best practice 10. Dynamic application security testing (DAST) using Veracode For subprocessor AWS, visit the AWS security page (https://aws.amazon.com/security/). Strong encryption is used for data in transit and at rest. These features include: • Data encryption capabilities available in AWS storage (S3 Amazon Simple Storage Service) and database service (RDS Amazon Relational Database Service). • AWS Key Management to secure access to APIs.

Additional Details

Record (GDPR Ref)	
Automated decision making or profiling performed on data? (Art 13 (2)(f))	N/A
Purpose of automated decision making or profiling (if applicable) (Art 13 (2)(f))	N/A

About This ROPA Entry Information document

The information provided that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

V. 1.0 Nov 22