PiQASO

PiQASO Deliverable 1.2

Grant Agreement	101190366
Project Title	DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Project acronym	PiQASO
Project Start Date	01 January 2025
Number of Deliverable	D1.2
Report Title	Data Management Plan
Related Work Package	WP1
Related Task	T1.2
Lead Organization	QUBI
Submission Date	30 June, 2025
Last Change Date	30 June, 2025
Dissemination Level	Public

EUROPEAN PARTNERSHIP

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Abstract

This document constitutes the Data Management Plan (DMP) of the PiQASO project, describing the data management life cycle for the data to be collected, processed and/or generated by a Digital Europe project. The overall aim of our data management strategy is to make research data findable, accessible, interoperable and re-usable (FAIR).

The DMP provides an analysis of the main elements of the data management policy that are used by the consortium with regards to all data that is collected and generated within the project. According to the European Commission's Guidelines on Data Management, the DMP will address data set reference and name, data set description, standards and metadata, data sharing, archiving and preservation on a dataset by dataset basis. A first version is submitted during M06 of the project and any occurring further updates in this respect will be provided during the project lifespan, on the basis of the actual developments of the technical work. The DMP ensures that all output is managed and maintained and that the data produced by the project is subject to appropriate levels of security, including the EU General Data protection Regulation (GDPR).

This document has been compiled as a summary of an information collector-based survey, according to the *EC Guidelines on FAIR Data Management in Horizon 2020* [1] and the FAIR Guiding Principles for scientific data management and stewardship [2]. Special consideration was given to the fact that the software is fundamental and vital part of research data, yet faces significant challenges for searchability, productivity, quality, reproducibility, and sustainability"[3].

This first version of the DMP mainly focuses on a synopsis of data management in PiQASO in a top-down approach. After describing the project system information flow and providing a general overview of PiQASO data, the guidelines and provisions for making data FAIR are described. The final sections of the document cover sharing, archiving and preservation of data, as well as data security.

Since it is early in the project, more detailed concepts of information exchange and data preservation will follow in the course of the project lifetime. The PIQASO consortium is aware of these aspects and will tackle them by updating the present document accordingly at a later stage. Therefore, information in this document is subject to change and updates will be included in the periodic reports or during the project lifetime whenever necessary.

Authoring & approval

Author(s) of the document

Name (Organisation name)	Date
Stylianos Kazazis (QUBITECH)	25/06/2025
Symeon Tsintzos (QUBITECH)	15/06/2025
Savvoula Oikonomou (UBITECH)	03/06/2025
Vassilis Kalos (UBITECH)	15/06/2025

Reviewed by

Name (Organisation name)	Date
Antonis Michalas (TAU)	20/06/2025
Angelina Katsifaraki (NCIS)	20/06/2025

Document history

Version	Date	Contributor/Organisation	Additional information
0.1	28/04/2025	QUBITECH	ToC created, Request for partners' input
0.2	03/06/2025	UBITECH	V0.2 doc populated with input
0.3	04/06/2025	UBITECH	Added information on Digital Europe program
0.4	06/06/2025	QUBITECH	Updates on Chapter 2
0.5	09/06/2025	QUBITECH	Updates on Chapters 3, 4 and 5
0.6	15/06/2025	QUBITECH	Updates on Chapters 6, 7, 8 and 9
0.7	17/06/2025	QUBITECH	Final version, ready for internal review
0.8	18/06/2025	QUBITECH	Release for internal review
0.9	25/06/2025	QUBITECH	Internal Review, Addressing reviewers' comments
1.0	30/06/2025	UBITECH	QA review and submission

PiQASO

Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

The project funded under Grant Agreement No. 101190366 is supported by the European Cybersecurity Competence Centre

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.”

Table of contents

List of figures

List of tables

List of acronyms

Acronym	Description
API	Application Programming Interface
DMP	Data Management Plan
DoA	Description of Action
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
SME	Small Medium Enterprices
TLS	Transport Layer Security
UE	Users Equipment

1 Introduction

1.1 Scope and Purpose

The current digital infrastructure prevents research and development from achieving their most productivity. While datasets resulting from research are often made publicly available, they: a) frequently go undocumented, b) are provided in non-standard formats, and c) are not uniquely identified, or are hardly accessible. This makes it hard to collect and compare results from several projects using automated methods. It is thus important to take data management into account from the beginning of projects, so that these limitations are overcome. The main goal of this document is to identify the datasets that will be produced during the PiQASO project, research on which standards might be employed to potentiate their reusability and analyse up to which extent they might be disseminated. Overall, the produced datasets will be a result of different technologies and cryptographic schemes being applied across different layers of the compute continuum, ranging from user equipment (UE) and network elements to infrastructure and cloud elements.

More concretely, this plan describes the **data management life cycle for all data sets that will be collected, processed or generated by the research project**. It is a document outlining how research data will be handled both during the research project and after it is completed, describing **what data will be collected, processed or generated and following what methodology and standards, whether and how this data will be shared and/or made open, and how it will be curated and preserved**.

The Data Management Plan (DMP) is required element for any EU funded project, such as *Horizon Europe* and *Digital Europe* projects. This DMP has been identified in the Description of Action (DoA) as deliverable D1.2. It is drafted according to the *FAIR Data principles* outlined in the Data Guidelines for Open Research Europe [4]. The main goal of the DMP is to ensure that PIQASO's research data is *FAIR* – *F*indable, *A*ccessible, *I*nteroperable and *R*e-usable.

It should be noted that the DMP is intended to be a living document. It will be periodically revised to reflect changes in the data that may be provided by the project and to share additional information on the datasets.

This first version of the PiQASO DMP has been written at an early stage of the project. In this stage, the consortium partners have started to develop a mutual understanding of the PiQASO system functionalities. Therefore, an overview of the data to be created is provided in this document, as well as general guidelines and processes for the handling of research data. Detailed information will be subject of later versions of the DMP updated during the periodic reviews.

All partners have contributed to this document, particularly through a comprehensive DMP information collector. The methodology behind this approach is described in Chapter 2. A summary of these results is provided in Chapter 3, while Chapter 4, Chapter 5, Chapter 6 and Chapter 7 and 8 describe the data management, accessibility, security and ethical measures.

The present report forms a deliverable -primarily- addressed to:

- European Commission
- Partners of the PiQASO project
- EU Parliament

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Digital Europe, Horizon Europe projects and other Post-Quantum Cryptography (PQC) related projects (clustering activities)

- Organizations and experts involved in the PiQASO case studies.

- Other relevant organizations both public and private, including associations of relevant stakeholders

1.2 Scope and Purpose Relation to other WPs and Deliverables

The delivery of the present document falls under Work Package (WP) 1 activities and specifically Task 1.2, which extends until M36 of the PiQASO project. In the context of the related activities, it is, thus, intended that the DMP is a living document, subject to updates -to the extent necessary- based on the progress of the project activities. It should be noted that a detailed description of the data management practices concerning -in particular- processing of personal data in the context of webinars, surveys and questionnaires provided under WP1,T1.3 will be documented in the relevant periodic reporting supporting material. Also, DMP, is strongly related with all WPs of PiQASO project since it supports the data management life cycle for all research data that will be collected, processed, or generated within the project.

2 Data Management in Digital Europe

According to the European Commission (EC) all project proposals submitted to “Research and Innovation actions”, “Innovation actions”, “Coordination support actions” or any relevant schemes have to include a section on research data management which is evaluated under the criterion 'Impact'.

Data Management Plans (DMPs) are a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a EU funded project. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research.

The purpose of a DMP is to provide a discussion of the main elements of the data management policy that will be used by the applicants with regard to all the datasets that will be generated by the project.

Research data	Research data is the evidence that underpins all research conclusions (except those which are purely theoretical) and includes data that have been collected, observed, generated, created or obtained from commercial, government or other sources, for subsequent analysis and synthesis to produce original research results. These results are then used to produce research papers and submitted for publication.
Open research data	Openly accessible research data can typically be accessed, mined, exploited, reproduced and disseminated, free of charge for the user.
Secondary data	Secondary data are data that already exist, regardless of the research to be conducted.
Open access	Open access is understood as the principle that research data should be accessible to relevant users, on equal terms, and at the lowest possible cost. Access should be easy, user-friendly and, if possible, Internet-based.
Metadata	Metadata is data used to describe other data. It summarizes basic information about data, which can make finding and working with instances of data easier.
Research data repositories	Research data repositories are online archives for research data. They can be subject based/thematic, institutional or centralized.

Table 1: Clarification of Terms

Overall, having considered all relevant principles regarding lawful processing of personal data, scientific research data should be easily discoverable, accessible, assessable and intelligible, useable beyond the original purpose for which it was collected and interoperable to specific quality standards.

Towards that direction, the PiQASO’s Data Management also follows the Guidelines on FAIR Data Management in Horizon 2020 (**Error! Reference source not found.**), released by the

European Commission Directorate – General for Research & Innovation and are also applicable here.

The document addresses the following issues to be addressed: (i) Data Summary, (ii) FAIR Data, (iii) Allocation of Resources, (iv) Data Security, and (v) Ethical Aspects. Each of the previously defined has its own set of questions that has to be addressed. The proposed document states that it is not required to provide detailed answers to all the questions of the DMP that needs to be submitted by month 6 of the project, subject -also- to potential future updates. Rather, the DMP is intended to be a living document -to the extent necessary- in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur.

2.1 Alignment with Digital Europe and ECCC Data Governance Requirements

The PiQASO project, funded under the **DIGITAL-ECCC-2024-DEPLOY-CYBER-06** call, acknowledges the evolving data governance framework established under the **Digital Europe Programme (DEP)**, the **European Cybersecurity Competence Centre (ECCC)**, and associated EU legislative instruments, including the **Data Governance Act (DGA)** and the upcoming **AI Act** (where applicable to AI-driven components within the PIQASO framework).
In addition to following the **FAIR Data Principles** traditionally associated with Horizon Europe, PiQASO extends its data management practices to align with the specific operational and legal obligations introduced by Digital Europe:

- **Cross-border Data Interoperability:** PiQASO's data management model ensures that data formats, models, and interfaces used within the project (e.g., NETCONF/YANG, OpenAPI specifications) comply with recognized open standards and are compatible with **European data spaces and cross-border services** promoted under the Digital Europe framework.
- **Data Sharing Governance:** The project commits to the principles of lawful, secure, and transparent data sharing, aligned with the **Data Governance Act (Regulation (EU) 2022/868)**. Data intended for external sharing, whether public or restricted, will adhere to appropriate **data intermediation services or trusted data-sharing protocols** where applicable, particularly for sensitive cybersecurity threat data and trusted path telemetry data.
- **Cybersecurity Data Handling Standards:** As a DIGITAL-ECCC action, PIQASO aligns its data security framework with **ENISA's recommendations on cybersecurity data governance** and the **European Cybersecurity Certification Framework**. Data exchanged within and beyond the consortium will comply with best practices for secure data flows, integrity assurance, and access control across distributed infrastructures.
- **AI Act Provisions (if applicable):** In cases where PIQASO technical artifacts involve AI-driven threat detection, telemetry analytics, or optimization engines, the project will proactively assess and document their compliance readiness under the provisions of the proposed **AI Act (COM/2021/206 final)**, particularly with regard to data quality, traceability, and security obligations for high-risk AI systems.

This alignment ensures that PiQASO's data management strategy not only adheres to FAIR and open science principles but is also compatible with the emerging **European data governance landscape** for operational digital infrastructures, thus supporting future integration and sustainability of project results within the **European Cybersecurity Community**.

3 PiQASO Data Management Overview

As described in the Guidelines on FAIR Data Management that should be followed by any EU funded project, a Data Management Plan is a key element to ensure data is well managed. For this reason, in this section we will first identify the type of artefacts that will be generated and collected in the framework of the project. During the lifetime of the PiQASO project, several artefacts will be produced. The artefacts that will be collected/generated are listed below in Section 3.2. As the project evolves, this list may require modifications (addition or removal of artefacts) with respect to the project developments.

3.1 Types and Formats of Artefacts Generated/Collected

In order to provide an overview of the different data sets that are currently available and are planned to be produced in the PiQASO project, the following table shows the data type, the related WP number and the format, in which the data will be presumably stored.

#	Artefact type	Explanation	WP#	Format (indicative)
1	Research Item	Models and Meta models, Policies, Questionnaires, Deliverables, Papers	2-6	.xls, .csv, .txt, .docx, .pdf
2	Software	Code, APIs, microservices, libraries, PQC Awareness Academy’s dashboard	2-5	.xls, .csv, .txt, .docx, .pdf, .ccp, .h
3	Dataset	Synthetic, dummy	2-5	.xls, .csv, .txt, .docx, .pdf

Table 2: PiQASO’s Artefacts overview

3.2 PiQASO Artefacts and Access

In the survey contacted during the first months of the project, the input collected from most of the partners is depicted in the following chart (Figure 1). The types of PiQASO Artefacts are distributed as 41% being datasets, 21% research items and the remaining 38% is of a software artefact type.

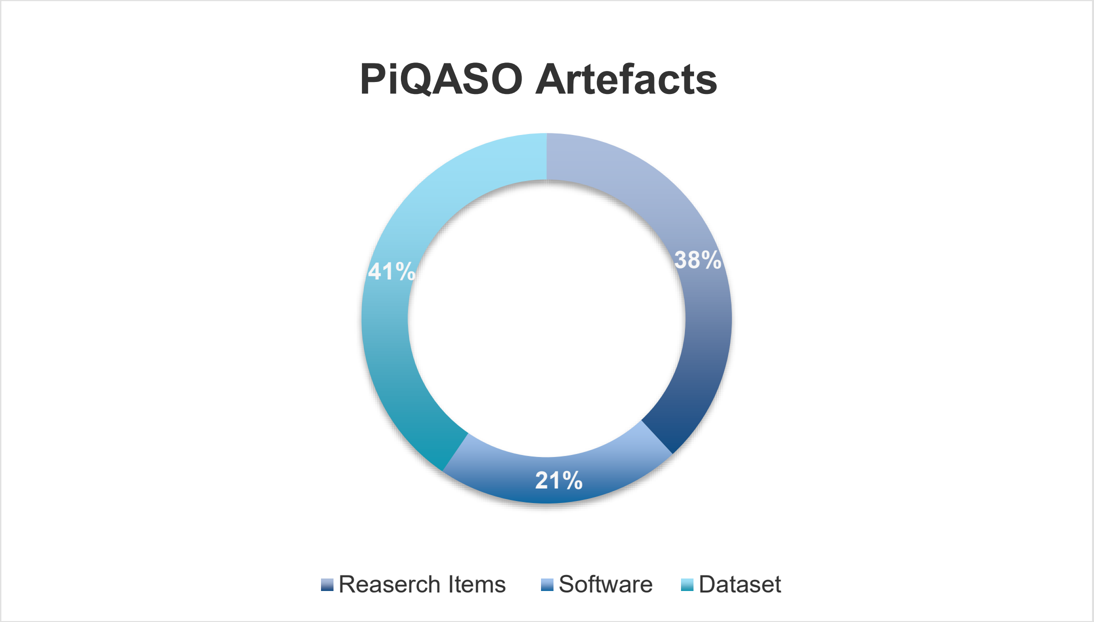


Figure 1: PiQASO artefacts' types

3.2.1 Research Items

The following table (Table 3) present the current status and consensus within the Consortium with regards to the current identified research items and their access rights. It is provisioned that this table is a recurring exercise and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is monitored regularly.

Partner	Artefact Description	Publishable (P)/Non-Publishable (N-P)	Format
UBITECH	Scientific publications	P	.docx, .pdf
UBITECH	Deliverable D2.1	P	.docx, .pdf
UBITECH	Deliverable D3.2	P	.docx, .pdf
QUBITECH	Scientific publications	P	.docx, .pdf
QUBITECH	Deliverable D3.3	P	.docx, .pdf
QUBITECH	Deliverable D4.4	P	.docx, .pdf
TAU	Scientific publications	P	.docx, .pdf
TAU	Deliverable D2.2	P	.docx, .pdf
TAU	Deliverable D3.1	P	.docx, .pdf
UNIS	Deliverable D4.1	N-P	.docx, .pdf
UNIS	Deliverable D4.2	N-P	.docx, .pdf
K3Y	Deliverable D5.1	P	.docx, .pdf
K3Y	Deliverable D5.2	P	.docx, .pdf
PLURIBUS	Deliverable D5.3	P	.docx, .pdf
PLURIBUS	Deliverable D4.1	P	.docx, .pdf
UniBwM	Deliverable D4.3	P	.docx, .pdf
RAL	Scientific publications	P	.docx, .pdf

Table 3: Partners' Research Item provision

3.2.2 Software

The following tables present the current status and consensus within the Consortium with regards to the current identified artefacts of software type provided in the context of PiQASO project, along with relevant information accompanying them (Artefact description, Dataset description, Format/Type, End user, Existence of similar data, Possibility of integration and reuse, Standards and metadata, Data sharing, Archiving and preservation). As stated previously, it is provisioned that the tables presented in this subsection are recurring exercises and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is monitored regularly.

3.2.2.1 PiQASO PQC-as-a-Service (PQC-asaS)

Owner	QUBITECH, UBITECH, UniBwM
Artefact Description	PQC-asaS modality providing quantum-safe encryption, authentication, and authorization functionalities through a cloud-based, application-layer microservice, allowing even legacy or resource-constrained systems to offload computationally intensive PQC operations, while enabling crypto-agility, granular access control, and secure data sharing without requiring specialized hardware on the client side.
Dataset description	Go/TypeScript -based libraries and APIs
Format/Type	Code
End user	Users of the PiQASO framework
Existence of similar data	Partially for other types of crypto as a service concepts and interfaces
Possibility of integration and reuse	Should be deployed/reused on any legacy infrastructure
Standards and Metadata	Developers documentation (Sphinx), Source Code documentation (Doxygen)
Data Sharing	It hasn't yet been agreed up to what extent and under which open-source license the code will be made available
Archiving and preservation	Partner private repository

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3.2.2.2 PiQASO PQC Software Library

Owner	UBITECH, QUBITECH, UniBwM, TAU, BYTE
Artefact Description	SW stack including reference implementations of lattice- and hash-based crypto algorithms (Kyber, Dilithium, FALCON, SPHINCS+). To be used as the basis for PiQASO's secure implementation of PQC Ensemble featuring a fully-fledged (SW) optimization and acceleration design space.
Dataset description	C/C++ and/or Go-based libraries
Format/Type	Code
End user	Users of the PiQASO framework
Existence of similar data	Partially for other types of PQC libraries
Possibility of integration and reuse	Should be deployed/reused on any compatible device
Standards and Metadata	Developers documentation (Sphinx), Source Code documentation (Doxygen)
Data Sharing	It hasn't yet been agreed up to what extent and under which open-source license the code will be made available
Archiving and preservation	Partner private repository

3.2.2.3 PiQASO Quantum Resistant-Trusted Computing Base (QR-TCB)

Owner	UBITECH, QUBITECH
Artefact Description	PQC-enabled Trusted Computing Base providing a secure, isolated environment for executing primitives from the PQC SW library, supporting both contemporary and PQ cryptography and ensuring cross-platform interoperability through extensions to the GlobalPlatform API
Dataset description	N/A
Format/Type	Code
End user	Users of the PiQASO framework
Existence of similar data	ARM Trustzone, Intel SGX

Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardized tools such as Doxygen.
Data Sharing	It hasn't yet been agreed up to what extent and under which open-source license the code will be made available
Archiving and preservation	Partner private repository

3.2.2.4 PiQASO Crypto Assessment & Conformance Toolkit

Owner	**RAL, UBITECH, QUBITECH**
Artefact Description	(Semi)-Automated tool for monitoring and identifying the crypto algorithms used by an infrastructure and identifying possible weaknesses through mutation-based fuzzing. Used as the basis for monitoring the cryptographic posture of legacy systems (on-boarded by use case partners), identify possible vulnerabilities and facilitate the planning and conformance to PQC.
Dataset description	C/C++-based libraries and APIs
Format/Type	Code
End user	Users of the PiQASO framework
Existence of similar data	AppViewX AVX ONE, IBM Z Crypto Discovery and Inventory
Possibility of integration and reuse	Should be deployed/reused on any legacy infrastructure
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardized tools such as Doxygen.
Data Sharing	It hasn't yet been agreed up to what extent and under which open-source license the code will be made available
Archiving and preservation	Partner private repository

3.2.2.5 PiQASO Academy Online Platform

Owner	K3Y
Artefact Description	A unique academy that will gather a set of PQC-related courses. The academy will also include webinars, training videos and workshops focusing on the readiness levels and current knowledge on PQC and CyberSecurity aspects.
Dataset description	Moodle-based e-learning Platform
Format/Type	Code
End user	Non-tech executives, Intermediate users, Tech experts (from SMEs, industry and research community), Users of the PiQASO framework
Existence of similar data	IBM Quantum Learning Platform, NIST PQC Project Portal
Possibility of integration and reuse	The platform contains reusable content for any stakeholder relevant to PiQASO framework
Standards and Metadata	SCORM, LTI
Data Sharing	A basic code version will be publicly available
Archiving and preservation	Partner private repository

3.2.2.6 PiQASO Integration APIs

Owner	NCIS
Artefact Description	APIs designed to extend TLS handshake negotiation to support both PQC and legacy cryptographic algorithms.
Dataset description	RESTful API, JSON for data interchange, HTTP/HTTPS protocols
Format/Type	Code
End user	Developers and systems integrators involved in the PiQASO project
Existence of similar data	No direct similar data

Possibility of integration and reuse	Designed to integrate with existing TLS implementations and adaptable for future cryptographic standards
Standards and Metadata	Follows RESTful standards, JSON Schema for data structure, OpenAPI for documentation
Data Sharing	Limited to PiQASO stakeholders and authorized partners
Archiving and preservation	Partner private repository after the end of the project.

3.2.2.7 PiQASO ROS 2 Integration

Owner	**PAL**
Artefact Description	Integration of PiQASO into the ROS 2 framework's communication protocol (DDS), both using it asaS or directly through client libraries. This will allow for quantum-safe authentication and encryption of ROS 2 topics, services and actions.
Dataset description	C++-based libraries
Format/Type	Code
End user	ROS 2 users
Existence of similar data	TLS over TCP already implemented in ROS 2 DDS implementation.
Possibility of integration and reuse	The TLS support is embedded into the DDS implementation, but the actual integration of a new encryption mechanism may prove challenging.
Standards and Metadata	Developers documentation (Sphinx), Source Code documentation (Doxygen)
Data Sharing	Open source license, either MIT or Eclipse, as per CycloneDDS and ROS 2.
Archiving and preservation	Partner private repository.

3.2.2.8 MONITOR Gateway

Owner	PARTICLE
Artefact Description	The MONITOR Platform is a remote patient monitoring system that includes the capability to monitor the pre-hospital assistance being provided to patients while en-route to the hospital. In PiQASO, MONITOR will support the use case, allowing the secure exchange of relevant data concerning the ambulance transport service and the patients' health information between the ambulance and the destination hospital. For this purpose, a MONITOR gateway (hardware component, linux-based, running MONITOR client components), installed on the ambulance, will be used. The gateway connects the ambulance devices to the MONITOR Platform.
Dataset description	N/A
Format/Type	JSON
End user	PiQASO Researchers
Existence of similar data	Unique to the MONITOR Platform
Possibility of integration and reuse	The MONITOR data may be provided to other systems
Standards and Metadata	HL7 FHIR
Data Sharing	The MONITOR data will be provided through an API to the PiQASO partners to support the security and privacy analyses conducted in the project.
Archiving and preservation	Partner private repository.

3.2.2.9 TelluCare Remote Patient Monitoring

Owner	TLU
Artefact Description	Software to manage medical devices and allowing patients to perform measurements applying the medical devices, and providing measurements and other patient data inputs to the right health personnel for follow up patients remotely. Provide features for video meetings and chatting between patients and health personnel.
Dataset description	N/A

Format/Type	Code
End user	Users of the PiQASO framework
Existence of similar data	Unique to the TelluCare Platform
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	Data is structured according to the HL7 FHIR standardised data model
Data Sharing	Test data sets will be openly available for the Entrust partners. May consider to apply existing openly available FHIR based datasets.
Archiving and preservation	Partner private repository. Potentially openly available repositories of relevant FHIR datasets

3.2.3 Dataset

The following tables present the current status and consensus within the Consortium with regards to the current identified artefacts of dataset type provided in the context of PiQASO project, along with relevant information accompanying them (Dataset description, Format/Type, End user, Existence of similar data, Possibility of integration and reuse, Standards and metadata, Data sharing, Archiving and preservation). As stated previously, it is provisioned that the tables presented in this subsection are recurring exercises and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is monitored regularly.

3.2.3.1 PiQASO (system) requirements, use cases (system) Architecture

Owner	**UBITECH**
Dataset description	These documents describe the requirements of the PiQASO framework and the use-case system architecture and will establish concrete goals for the remainder of the project
Format/Type	.docx
End user	The PiQASO documentation will be made available to the public so that other groups may contribute to the project or take advantage of it
Existence of similar data	N/A

Possibility of integration and reuse	The system requirements and architecture may be used as a basis for other projects on PQC in various application domains
Standards and Metadata	Experimental results will be published under the form of a Word file.
Data Sharing	The documentation will be made publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners' private and public repositories

3.2.3.2 Crypto Assessment & Conformance Toolkit output

Owner	**RAL, UBITECH**
Dataset description	Lists of existing cryptographic assets per infrastructure (use case), encapsulating digital certificates, cryptographic keys, algorithms, and protocols used to secure data and systems.
Format/Type	XML, JSON, and Protocol Buffers
End user	Users of the PiQASO framework
Existence of similar data	From similar crypto asset discovery tools
Possibility of integration and reuse	Relevant to the use cases application domains
Standards and Metadata	Results may be published under the form of XML, JSON, and Protocol Buffers files.
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners private and public repositories

3.2.3.3 PQC migration checklists

Owner	**PLURIBUS**
Dataset description	Formulation of sector-dependent migration checklists and plans, enabling organizations to effectively transition from traditional cryptographic methods to PQC solutions, ensuring a seamless and secure adaptation to the quantum era.
Format/Type	.docx, .pdf

End user	PiQASO use case partners
Existence of similar data	EVERTRUST white paper, PQCC Post-Quantum Cryptography Migration Roadmap
Possibility of integration and reuse	Stakeholders from diverse sectors, including government agencies, industries (automotive, finance, healthcare, aerospace, online media, UAVs, transportation, and other industrial sectors)
Standards and Metadata	Migration checklists will be published under the form of a .docx file or similar formats
Data Sharing	Publicly available through PiQASO Academy and/or Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners private and public repositories

3.2.3.4 PQC-related Courses and Training Modules

Owner	**WP5 Contributors**
Dataset description	A collection of well-structured e-learning materials including webinars, videos and presentation slides
Format/Type	.mp4 , .pdf , .pptx , .txt , .srt , .md , .zip , .csv , .json
End user	PiQASO partners, Non-tech executives, Intermediate users, Tech experts (from SMEs, industry and research community)
Existence of similar data	IBM Quantum Learning Platform Courses , QC and PQC Training by Tonex , MIT OpenCourseWare , Post-Quantum Cybersecurity Training Program by UMBC
Possibility of integration and reuse	High, since practitioners from research, government and organizations can easily interact with such content
Standards and Metadata	IEEE LOM (1484.12.1-2020) , LRMI
Data Sharing	Data will be available through PiQASO Academy
Archiving and preservation	Partner private and public repository

3.2.3.5 Integrated System Logs

Owner	**NCIS**

Dataset description	Timestamped records of the system operation generated automatically to document system events, activities or incidents.
Format/Type	.txt/.json/.csv
End user	PiQASO partners
Existence of similar data	N/A
Possibility of integration and reuse	The dataset can be used for system performance & security analysis.
Standards and Metadata	This remains to be decided.
Data Sharing	PiQASO CI/CD tools
Archiving and preservation	Project lifecycle

3.2.3.6 Experimental Measurements

Owner	**UBITECH, QUBITECH, TAU, UniBwM, BYTE**
Dataset description	Security-relevant (e.g. Key management logs) and operational datasets (e.g. token and session metadata) are generated, especially given the role in handling authentication, encryption, and access control
Format/Type	.csv
End user	Experimental results may be included in scientific publications.
Existence of similar data	Performance metrics are typically included in scientific publications where PQC schemes are considered.
Possibility of integration and reuse	The results may be used in other publications for performance comparisons.
Standards and Metadata	Experimental results will be published under the form of a CSV file or similar formats
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners private and public repositories

Owner	PAL
Dataset description	Performance benchmarking of ROS 2 using different encryption and authentication protocols.
Format/Type	.csv, .json
End user	PiQASO partners and the ROS 2 community.
Existence of similar data	The benchmarks only compare different DDS implementations.
Possibility of integration and reuse	High, we have flexible benchmarking tools at PAL.
Standards and Metadata	ROS 2 Rosbags (mcap), CSV and similar formats.
Data Sharing	Github, ROS 2 forums
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners private and public

Owner	ABINSULA, MOH, MORE, CERTH, TLU, BIBA, NEDHO, DPG, FGC, STROWL
Dataset description	PQC-relevant benchmarking data extracted during the use case execution.
Format/Type	.csv, .json
End user	Experimental results may be included in scientific publications.
Existence of similar data	Performance metrics are typically included in scientific publications where PQC schemes are considered.
Possibility of integration and reuse	The results may be used in other publications for performance comparisons.
Standards and Metadata	Experimental results will be published under the form of a CSV file or similar formats
Data Sharing	Publicly available through Zenodo or Gitlab

Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners private and public

3.2.3.7 Use case Datasets

Owner	**PARTICLE**
Dataset description	Security-relevant synthetic IoT-based datasets are generated as part of the use cases to identify vulnerabilities at the system and device levels.
Format/Type	JSON
End user	PiQASO Researchers
Existence of similar data	N/A
Possibility of integration and reuse	The dataset will be used to support the security analysis conducted as part of the project.
Standards and Metadata	Experimental results will be published under the form of a Word file.
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The dataset will be published in the project's repository.

Owner	**ACCELI**
Dataset description	The data fusion and object detection /identification algorithms collect data from sensors (e.g. LiDAR, Camera and UAV), fuses them and send the output results to the PiQASO backend, if needed. Security-relevant and operational datasets are generated regarding the pilot authentication, encryption and access between the UAV and the Ground Station. For the execution of the flights the PX4 flight control will be used, which is an open source autopilot software.
Format/Type	JSON
End user	Experimental results may be included in scientific publications.
Existence of similar data	Application domain-specific performance metrics are typically included in scientific publications

Possibility of integration and reuse	PiQASO UAV will collect video data through its embedded camera and raw data from the embedded sensors. It will receive notifications and commands from C2 and it will transmit the outcomes from the edge processing to C2
Standards and Metadata	RSTP, XML, JSON
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The dataset will be published in the project's repository.

Owner	**CXB**
Dataset description	Security-relevant and operational dataset (e.g. A10 logs) are generated to monitor external traffic and encryption data. A first version of this dataset will be synthetic and anonymized while a second version of this dataset could be with real data if the dataset doesn't leave CXB's premises.
Format/Type	.csv,.json
End user	N/A
Existence of similar data	Application domain-specific performance metrics are typically included in scientific publications
Possibility of integration and reuse	The dataset will be used to support the security analysis conducted as part of the project.
Standards and Metadata	Experimental results will be published with the agreed format, nevertheless, the data used for the training will be considered sensible.
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The dataset will only be preserved as long as it is needed for the project, once its purpose has been accomplished, the dataset will be eliminated. On the other hand, the results and conclusions from this dataset will be published in the project's deliverables

3.3 Expected size of the data (if known)

It is expected that the project will generate research datasets (i.e. results of the technologies, services of the demos, etc.), publications, new services proposal, dissemination material, etc as an outcome of its research activities. Due to size of the project, scope of work and complexity, the expected size cannot be confidently estimated at the moment.

4 PiQASO ORDP Participation

The Open Research Data Pilot (ORDP) of the European Commission enables open access and reuse of research data generated by Horizon Europe projects. There are two main pillars to the Pilot: a) developing a DMP and b) providing open access to research data.

A project that opts-in ORDP have to adhere to the following conditions:

- Develop (and keep up-to-date) DMP.
- Deposit the data in a research data repository.
- Ensure third parties can freely access, mine, exploit, reproduce and disseminate this data.
- Provide related information and identify (or provide) the tools needed to use the raw data to validate the research.

The ORDP applies to:

- The data (and metadata) needed to validate results in scientific publications.
- Other curated and/or raw data (and metadata) that are specified in the DMP.

From the current consensus within the consortium some of the PiQASO Artefacts will be publicly available as depicted in the graphics below (Figure 2, Figure 3 and Figure 4).

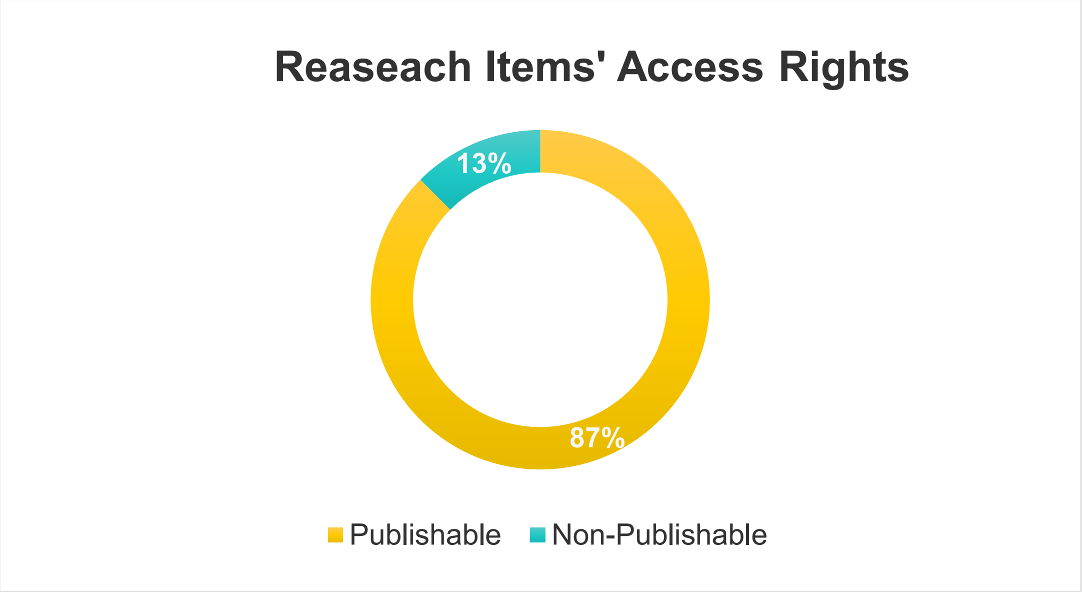


Figure 2: Access rights of the PiQASO project's research items.

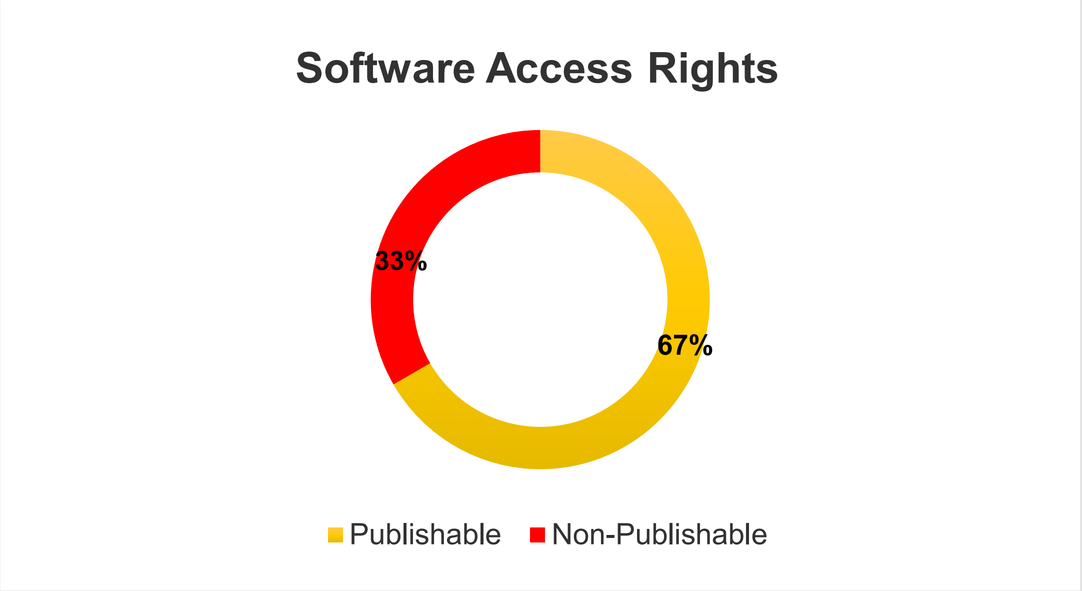


Figure 3: Access rights of the PiQASO project's software artefacts.

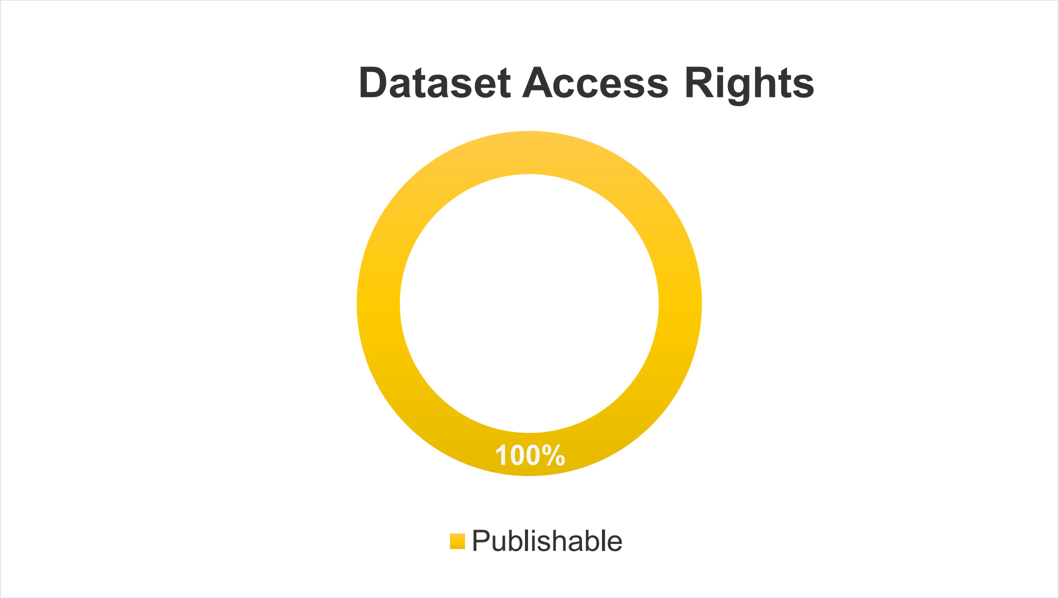


Figure 4: Access rights of the PiQASO project's datasets.

4.1 Data Excluded from ORDP

In case of data that is not expected to be made available in open access, it will be processed by project matters and internally retained by the relevant partners after the project. It will count with an agreement to make it available only for the purposes of validating the research, but not open access.

In case of restrictions, the consortium will count with some contact points available (e.g. e-mail address) that can be used to request data. The provision of requested data will be decided on a case-by-case basis considering relevant restrictions (software licenses, NDAs, etc.). However, this matter will be better clarified as part of the sustainability strategy of the project.

Besides that, the project follows the Regulation 2018/1725 which sets forth the rules applicable to the processing of personal data by European Union institutions, bodies, offices and agencies.

4.2 Publishing Infrastructure for Open Access

The PiQASO publication infrastructure consists of a process and several web-based publication platforms that together provide long-term open access to all publishable, generated or collected results of the project. The implementation of the project will be done in accordance with the applicable regulations at national and EU level and, especially, with the General Data Protection Regulation (GDPR) protection of personal data[1].

More specifically, there are no cases where personal data information or sensitive information of internet users is collected (IP addresses, email addresses or other personal information) or further processed.

In the potential future case where the PiQASO consortium will collect and/or further process personal data, this will be done in accordance with GPDR. Overall, it is aimed that PiQASO only collects and/or further processes personal data are necessary for the attainment of the project objectives.

Both the process and the used web-based platforms are described in the following subsections.

4.2.1 Publishing Process

The PIQASO partners will follow a simple, deterministic process that decides if a result in PiQASO must be published or not. The term result is used for all kind of artefacts generated during PiQASO like white papers, scientific publications, and anonymous usage data. Public means that the result must be published under the open access policy. Non-public means that it must not be published. For each result generated or collected during PiQASO runtime, the following questions must be answered to classify it:

Does the result provide significant value to others or is it necessary to understand a scientific conclusion?
If this question is answered with yes, then the result is classified as public. If this question is answered with no, the result is classified as non-public. Such a result could be code that is very specific to the PiQASO platform (e.g., a database initialization) which is usually of no scientific interest to anyone, nor does it add any significant contribution.
Does the result include personal information that is not the author's name?

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

If this question is answered with yes, the result is classified as non-public. Personal information beyond the name must be removed if it should be published. This also bears witness on the repetitive nature of the publishing process, where results which are deemed in the beginning as non-publishable can become publishable once privacy-related information is removed from them.

Does the result allow the identification of individuals even without the name?

If this question is answered with yes, the result is classified as non-public. Sometimes data inference can be used to superimpose different user data and reveal indirectly a single user's identity. As such, in order to make a result publishable, the information included must be reduced to a level where single individuals cannot be identified. This can be performed by using established anonymization techniques to conceal a single user's identity, e.g., abstraction, dummy users, or non-intersecting features.

Does the result include business or trade secrets of one or more partners of PIQASO?

If this question is answered with yes, the result is classified as non-public, except if the opposite is explicitly stated by the involved partners. Business or trade secrets need to be removed in accordance with all partners' requirements before it can be published.

Does the result name technology that is part of an ongoing, project-related patent application?

If this question is answered with yes, then the result is classified as non-public. Of course, results can be published after patent has been filed.

4.2.2 Publishing Platforms

In PiQASO, we use several platforms to publish our results openly. The following list presents the platforms used during the project and describes their concepts for publishing, storage, and backup.

Project Website (here):

The partners in the project consortium decided early to setup a project-related website. This website describes the mission and the general approach of PiQASO and its development status. A blog informs about news on a regular basis. Later in the project the developed PiQASO platform will be announced. A dedicated area for downloads is used to publish reports and white papers as well as scientific publications (in pre-camera ready form, or through links to the publisher’s websites in case these are not open access). All documents are published using the portable document format (PDF)[2]. All downloads are enriched by using simple metadata information, such as the title and the type of document. The website is hosted by partner UBITECH, whereas is moderated and regularly updated by partner PLURIBUS. All webpage-related data is backed up on a regular basis. All information on the project website can be accessed without creating an account. The website is backed up once per month.

Project Gitlab (here):

[2] Note that the site will not host spreadsheets. It exclusively host PDFs

GitLab is a well-established online repository which supports distributed source code development, management, and version control. It is primarily used for source code data. It enables world-wide collaboration between developers and provides also some facilities to work on documentation and to track issues. GitLab provides paid and free service plans. Free service plans can have any number of public, open-access repositories with unlimited collaborators. Private, non-public repositories require a paid service plan. Many open-source projects use GitLab to share their results for free. The platform uses metadata like contributors' nicknames, keywords, time, and data file types to structure the projects and their results. The terms of service state that no intellectual property rights are claimed by GitLab over provided material. For textual metadata items, English is preferred.

All source-code components that are implemented during this project and decided to be public will be uploaded to an open access GitLab repository.

Project Sharepoint (here):

SharePoint is a widely used collaboration platform developed by Microsoft, primarily designed for document management, content sharing, and team collaboration. It supports the creation of internal websites and repositories where organizations can store, organize, and share information securely. SharePoint facilitates both internal and external collaboration by enabling partners to work together on documents, track tasks, and maintain version control for content. The platform employs robust encryption methods and fine-grained access controls to protect sensitive data and ensure only authorized users have access. SharePoint does not claim ownership over user-generated content, and intellectual property rights remain with the respective users or organizations. The service relies on metadata like document properties, tags, and usage patterns to enhance search functionality and content organization.

Zenodo (here):

Zenodo is a research data archive / online repository which helps researchers to share research results in a wide variety of formats for all fields of science. It was created through EC's OpenAIRE+ project and is now hosted at CERN using one of Europe's most reliably hardware infrastructures. Data is backed nightly and replicated to different locations. Zenodo not only supports the publication of scientific papers or white papers, but also the publication of any structured research data (e.g., using XML). Zenodo provides a connector to GitLab that supports open collaboration for source code and versioning for all kinds of data. All uploaded results are structured by using metadata, like for example the contributors' names, keywords, date, location, kind of document, license, and others. Considering the language of textual metadata items, English is preferred. All metadata is licensed under CC0 license (Creative Commons 'No Rights Reserved'). The property rights or ownership of a result does not change by uploading it to Zenodo. All public results generated or collected during the project lifetime will be uploaded to the dedicated Zenodo community created for long-term storage and open access.

4.2.3 Access and Sharing

The accessing and sharing of data is firstly ruled by two documents: the non-disclosure agreement, which stipulates under which conditions transmitted information between the project partners is deemed confidential and must not be further disseminated; and the Description of Action (DoA) which stipulates the dissemination level of each deliverable.

Moreover, the project consortium will comply with the FAIR (findable, accessible, interoperable and reusable) (European Commission, 2016) guidelines of the Horizon Europe programme.

The data necessary to successfully complete the project WPs will be shared without any restrictions amongst the WP partners either via internal repositories or direct communication. Public data will be made available at the project's website or other repositories, as appropriate. Users will be made aware of this data primarily through research publications, patent applications, dissemination activities, invited talks, social networks and the project website. Data will be made available to the project consortium as soon as it is available; to standardization bodies when required; and to the public at the due date of the deliverable, and, in case a research publication is based on that, as soon as the paper is submitted (if submission is anonymous, this will be postponed). If access to confidential data is necessary by the public, restrictive measures will be put in place.

5 FAIR Data

PiQASO project supports the reuse of research data and follows FAIR principles [5]. FAIR represents a set of guiding principles to make data Findable, Accessible, Interoperable, and Reusable. The international FAIR Principles have been formulated as a set of guidelines for the reuse of research data. The acronym FAIR stands for findable, accessible, interoperable and reusable. Research data must be of quality that makes them accessible, findable and reusable.

Findable: data has a unique, persistent ID, located in a searchable resource, and documented with meaningful metadata.

Accessible: data is readily and freely retrievable using common methods and protocols, metadata is accessible even if the data is not.

Interoperable: data is presented in broadly recognized standard formats, vocabularies, and languages.

Re-useable: data has clear licenses, and accurate meaningful metadata conformity to relevant community standards and identifying its content and provenance.

5.1 Making Data Findable, Including Provisions for Metadata

This document launches the data management plan to support the effective collection and integration of the PiQASO data. Storage, processing and sharing (among project participants) will occur via data exchange platforms (such as Microsoft Sharepoint), whereas interaction with the wider public will be achieved through the official project website. Also, data will be stored at the coordinator’s repository and will be kept for minimum 5 years after the end of the project. Where requested, data will be kept for 2 more years.

A naming convention will include a concise description of contents, the host institution collecting the data and the month of publication.

Version numbering will only be an issue if a participant requests withdrawal of their data in which case a version number will be added to the filename.

No specific standards or metadata have been identified for the time being for the proposed datasets.

Data will be anonymized meaning that data will not identify any individuals and therefore real names of participants will NOT be distributed.

Data will be shared only in relation to publications (deliverables and papers). As such, the publication will serve as the main piece of metadata for the shared data. When this is not seen as being adequate for the comprehension of the raw data, a report will be shared along with the data explaining their meaning and methods of acquisition.

5.1.1 Discoverability of the data

In order to be able to use the data generated by the project it is essential to integrate data from the participants in the open calls and the activities undertaken by project partners. Taking into account the FAIR data principles [6] (meta)data should:

- Be assigned to a globally unique and persistent identifier;
- contain enough metadata to fully interpret the data, and;
- Be indexed in a searchable source.

By applying these principles data become retrievable and include their authentication and authorization details.

5.1.2 Data identification mechanisms

All documents associated to the project will be identified with the project name and unique and persistent document type designator and number that will be given to the coordinator for the submission to the EC. The version of the document should be part of the document name and title.

As per the documents related to project activities and/or deliverables, the tasks or deliverables number will be used to identify the document followed by a brief title of the activity or deliverable.

Example

PIQASO - D1.2 - Data Management Plan -v1.0.pdf

5.1.3 Naming conventions used

Each set of data produced (dataset, deliverables, etc.) will be named in a uniform way and will include a table with a version control.

The recommendations to name documents of the project are as follows [7]:

- Choose easily readable identifier names (short and meaningful)
- Do not use acronyms that are not widely accepted
- Do not use abbreviations or contractions
- Avoid Language-specific or non-alphanumeric characters
- Add a two-digit numeric suffix to identify new versions of one document
- Dates should be included back to front and include the four-digit years: YYYYMMDD.

For deliverables: **PIQASO _[Deliverable Code]-[Deliverable Title]_[Partner]-vA.BB** i.e.: PIQASO _D1.1-Project Handbook-v1.00 *(for submission to the Commission)*

For datasets: **WP [Work Package number] P [Pilot number; pilot activity number] - [description of the activity]** i.e.: WP4 P1.3 Results of demonstration performance.

5.1.4 Clear versioning of the documents

Only documents created by the consortium will be versioned, for this purpose templates include 3 descriptors to identify the versions and status of the documents:

Document history

Version	Date	Contributor/Organisation	Additional information
0.1			
0.2			

Table 4: Proposed document history table overview

Moreover, partners, following the recommendations included in section "Naming conventions" will identify the different versions by using a two-digit number following the descriptor Draft. A document reviewed by another partner should be returned to the principal author by including rev + acronym of the organisation. Only the principal author will change the draft number and will add the word FINAL to documents ready to be sent to the EC or those to be used as final versions.

The document history included in the document template should be filled in as follows:

Document history

Version	Date	Contributor/Organisation	Additional information
0.1	XX/XX/2025	ABC (CFG)	Section 2.1 needs to be completed
0.2	XX/XX/2025	CDE (KHM)	Section 2,1 completed. Comments added to the document.
0.3	XX/XX/2025	ABC (CFG)	Added suggestions by CDE

Table 5: Document history template - example

5.1.5 Standards for metadata creation (if any)

Basic metadata will be used to facilitate the efficient recall and retrieval of information by project partners and external evaluators and contribute to easily find the information requested. To this end, all documents related to the project have to include in the front-page information about author(s) & editor(s), WP, dissemination level and version.

To support the completeness of metadata, the project provides a metadata template to all stakeholders. The template will be a living document that might be expanded to fit project specific requirements.

#	Field	Description
1	Title	A name given to the resource.
2	Creator	An entity primarily responsible for making the resource
3	Subject	The topic of the resource
4	Description	e.g., abstract, table of contents, graphics, ...
5	Publisher	Only for published items.

6	Contributor	Entities that contributed to the making of the resource.
7	Date	The termination of the data collection period.
8	Type	[dataset, article, questionnaire, ...]
9	Format	File format of the resource.
10	Identifier	e.g., ISSN if your item has been published
11	Source	Which tools were used to collect the data
12	Language	A language of the resource.
13	Relation	A related resource.
14	Rights	Information about rights held in and over the resource.

Table 6: Metadata template for PiQASO datasets.

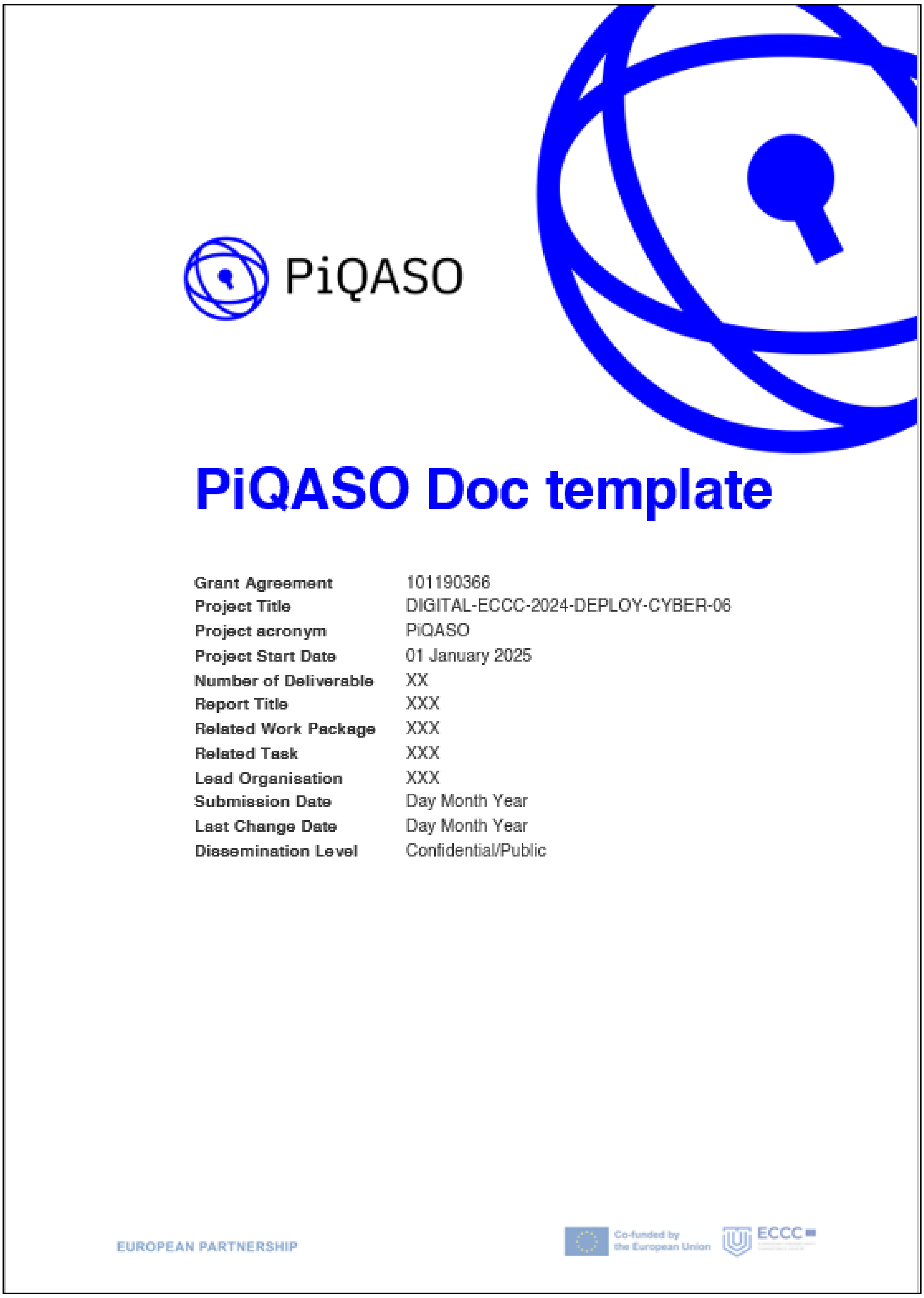
In addition to the dataset's metadata document, dataset providers are compelled to attach additional documents such as:

1. A description of the study
2. Method of research
3. Applied questionnaires
4. Data documentation / usage manual
5. Any other information that might be of interest to a data user

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE



PiQASO

PiQASO Doc template

Grant Agreement	101190366
Project Title	DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Project acronym	PiQASO
Project Start Date	01 January 2025
Number of Deliverable	XX
Report Title	XXX
Related Work Package	XXX
Related Task	XXX
Lead Organisation	XXX
Submission Date	Day Month Year
Last Change Date	Day Month Year
Dissemination Level	Confidential/Public

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ECCC

Figure 5:Template to be used for project documentation metadata overview

5.2 Making Data Openly Accessible

Where possible data will be made available subject to Ethics and participant agreement. However, the personally-identifiable nature of the data collected within PiQASO means that in most instances it would be difficult to release collected data. Where data is made available, we will do so using the Project's file repository hosted in coordinator's premises.

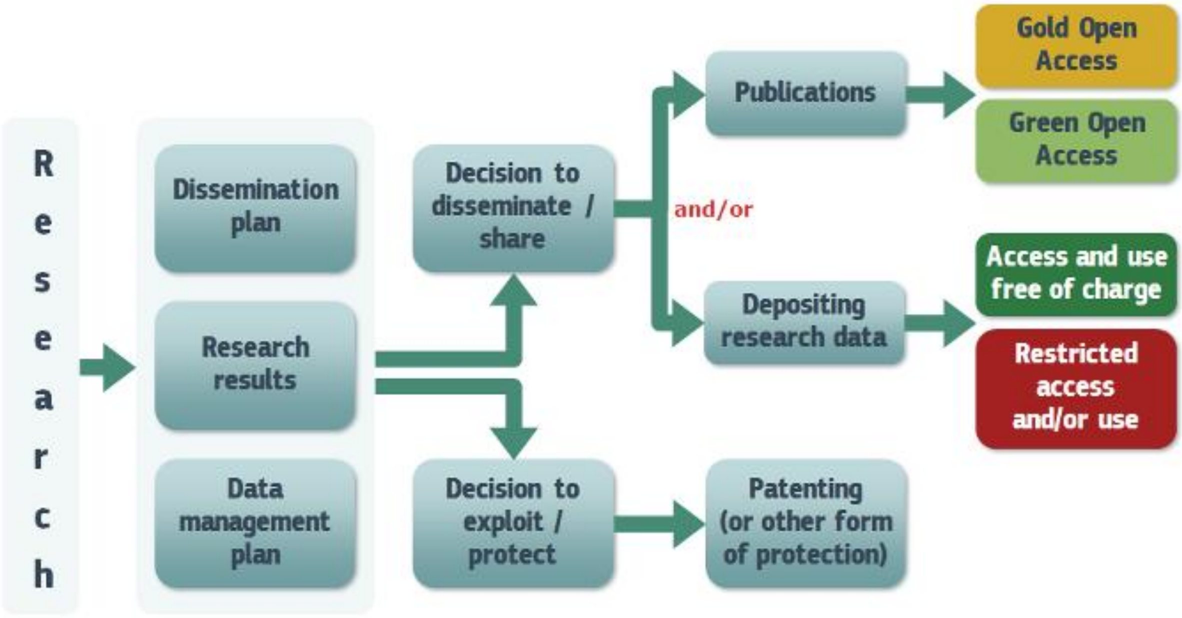

Research
Dissemination plan
Research results
Data management plan
Decision to disseminate / share
Decision to exploit / protect
and/or
Publications
Depositing research data
Patenting (or other form of protection)
Gold Open Access
Green Open Access
Access and use free of charge
Restricted access and/or use

Figure 6: Open access to scientific publication and research data in the wider context of dissemination and exploitation[3]

Prior to release, a requesting party will need to contact the Project Coordinator describing their intended use of a dataset. The Project Coordinator will send a terms and conditions document for them to sign and return. Upon return, the dataset will be released. Documentation will be included with the release of the data.

In alignment with the EC Guidelines on Open Access to Scientific Publications and Research Data in Horizon Europe, PIQASO will also follow a combination of Gold and Green Open Access strategy to its scientific publications, which will be agreed during the first months of the project execution. Gold Access will be encouraged for high-impact journal publications while the self-archiving, Green Access will be granted for the rest of the publications. The repositories listed in OpenDOAR, zenodo funded by OpenAIRE and the repositories available through the consortium members will be considered while there will also be a relevant repository on the website of the project and in social networking sites for scientists and researchers like ResearchGate.

5.2.1 Methods or software needed to access the data

[3] European Commission Directorate-General for Research & Innovation (2017) Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020

No specific software tools will be needed to access the data, since anonymous data sets will be saved and stored in word, pdf or excel to facilitate its exploitation and guarantee their long-term accessibility.

5.2.2 Deposit of data, associated metadata, documentation and code

Data will be deposited and secured on Microsoft Sharepoint file repository and additional instance of all data on coordinator's account.

5.3 Making Data Interoperable

The concept interoperable demands that both data and metadata must be machine-readable and that a consistent terminology is used.

5.3.1 Interoperability of data assessment

Partners will be responsible of storing the data in a comprehensive format and adapted to the real and current needs of the possible practitioners interested in using, merging or exploiting the data generated throughout the project. The assessment of data interoperability will be updated in future reviews in order to guarantee the PiQASO data fits the needs of a specific scenario such as data infrastructures, interests or purpose of data.

5.3.2 Vocabulary use

The vocabulary used in the project is a very standard and common language within the business creation culture and the logistics. Vocabulary won't represent any barrier for data interoperability a re-use.

5.4 Making Data Re-usable

For data to be re-usable, it is -generally- considered that meta(data) have a plurality of accurate and relevant attributes and that they are released with a clear and accessible data usage license. Moreover, it is considered that (meta) data are associated with their provenance and that they meet domain-relevant community standards.

Note that the overall management of knowledge and the provisioning for the establishment of the related Intellectual Property Rights is dictated in detail under PiQASO 's Grant Agreement and the consortium agreement stipulating -among other- for the ownership of the background and the foreground knowledge, as well as for the commercial exploitation of the project's results.

5.4.1 Increase data re-use through clarifying licenses

Data will only be available on project's Microsoft Sharepoint and their use will be restricted to the research use of the licensee and colleagues on a need-to-know basis. This non-commercial licence is renewable after 2 years, data may not be copied or distributed and must be referenced if used in publications. These arrangements will be formalised in a User Access Management licence which describes in detail the permitted use of the data.

5.4.2 Data quality assurance process

The project coordinator will be responsible of assuring the quality of the data by making sure dataset follow the FAIR principles included in this plan, and that data is updated.

Personal data processing will be done following the EU, national and international laws taking into account the "data quality" principles listed below [9] :

Data processing is adequate, relevant and non-excessive;

- Accurate and kept up to date;
- Processed fairly and lawfully;
- Processed in line with data subjects' rights;
- Processed in a secure manner;
- Kept for no longer that necessary and for the sole purpose of the project.

Data quality assurance process will be led in accordance with the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

5.4.3 Length of time for which the data will remain re-usable

The Consortium will contribute to maintain data re-usable as long as possible after the end of the project. A first period of 4 years has been established; however, this time can be extended under partners' agreement. This period can vary depending on the value of the data after the end of the project.

5.5 Artefact Template

The following tables try to capture the description of the data that will be produced in the context of PIQASO. Every use case will fill in such a template and subsequently all the templates will be collected with the beginning of WP4, the demonstration applications work package of the project.

Making data Findable	
Name of data set	*Universal identifier of the considered data [PIQASO_Wx_Tz_01]* *Please, provide one sentence description.*
Data types	*[Real time data stream, unstructured like tweets, synthetic data stream, log data of IDS, etc.]*
Data generation and/or collection	*Description of the type of input used to generate the data and the complete methodology and tools used for data collection*
Purpose	*What are the data collected/generated specifically used for?*
Data origin	*[Where applicable, information from applications to be developed by the partner.]*

Table 7: Making data findable template

Making data Accessible	
Accessibility	*Open/Confidential*
Repository	*Description/location of the available data.*
Shareability restrictions / related Information	*[Where applicable, information from applications to be developed by the partner.]*

Table 8: Making data accessible template

Making data Interoperable	
Format	*Data format, measuring unit, typical order of magnitude [JSON-like, CSV]*
Expected size of the data	*[To be defined, 3 TB/Day or 12 GB/day when compressed etc.]*
Standards and metadata[4]	*[The metadata attributes list. The used methodologies.]*
Standard software Interfaces	*List of the standards used to promote results replicability.*
Extensions to standard interfaces	*Extensions to the above standards as developed during the project.*

Table 9: Making data interoperable template

Making data Re-usable	
Re-use of existing data	*[No reuse of existing data, for the generation of synthetic datasets, it will be essential to create a recipe, reusing the existing data in logs etc.]*
Data types	*Consistent location of the data, including previous releases*
Data backup	*Constraints determining the quality/currency of the collected data.*
Quality Consistency	*Description/location of possible emulation tools useful for replicating the data*

Table 10: Making data re-usable template

[4] Note that the fields pertinent to standards are, also, relevant for reusability purposes.

6 Allocation of Resources

6.1 Data management responsibilities

Data will be stored at the Collaboration file repository (Microsoft Sharepoint), set by the Coordinator as the project's repository, and will be kept for 5 years after the end of the project. Where requested, data will be kept for 2 more years. The handling of the repository on behalf of PiQASO as well as all data management issues related to the project fall in the responsibility of the coordinator.

As for the publications, where the analyses of the empirical research data will be presented, the consortium will publish them in scientific journals that allow open access. The costs related to open access will be claimed as part of the Digital Europe grant.

Regarding the data resulting from the activities of the project, each WP leader will be responsible for the storage and compliance of the data and then for uploading in the PiQASO SharePoint web portal, or other storage systems to share the information of the project.

The PiQASO's coordinator assisted by the WP leaders will be responsible for updating this document and develop a strategy to encourage:

- the identification of the most-suitable data-sharing and preservation methods;
- the efficient use of data assuring clear rules on its accessibility;
- the quality of the data stored and
- the storage in a secured in a user-friendly interface.

6.2 Cost of potential value of long-term preservation

As stated in previous section, the costs of data storage and maintenance are not going to require extra funding once the project ends. As per the value of the data, it is important to take into account that the topics covered by the project respond to a current need of the logistics sector and customers' needs. Therefore, data coming out of this project will have a direct impact in the coming years but might not be of relevance as the challenges are being tackled or replaced by other priorities.

7 Data Security

PIQASO data exchange platform (Microsoft Sharepoint) applies technological and organizational measures to secure processing of personal data against publishing to unauthorized persons, processing in violation of the law and change, loss, damage or destruction.

- ***Information security***: Secure Socket Layer certificates are applied. In order to ensure the appropriate level of security, the password for the account will exist on the platform only in a coded encrypted form.

- ***Options for reading data***: The platform offers the possibility to make data available in a read-only or downloadable format, hindering the access to information by unauthorized users.

- ***Back-up policy***: Complete and redundant back-ups are done every week. Moreover, every time a modification is done an older version is saved.

- ***Accidental deletion or modifications***: In case of a catastrophic event that implies the partial or complete deletion of the data sets, the data from the most recent back up will be automatically restored (back-up won't be older than 60 minutes). In case of accidental deletion or modification only the most recent document will be restored, so in case of accidental changes or deletion data can be easily recovered.

- ***Deletion or modification of data by users***: Only administrators have the rights to delete or modify the information included in the datasets.

- ***Terms and conditions***: The Microsoft Sharepoint platform has specific terms of use and conditions that have to be accepted by all users of the platform.

8 Ethics Aspects

The PiQASO consortium is aware of the ethical aspects pertinent to the scope of PiQASO, which are addressed under the WP 1, Task 1.3 on “Quality, Risk and Ethics/Legal Management”.

The task is responsible for: a) Establishing and verifying quality standards for project achievements; b) Identifying, monitoring, and mitigating potential project risks; c) Ensure the legal & ethical compliance of the PiQASO (s/w, demonstrator & data to be generated) to the EU and national legislation (including GDPR). It will analyse the ethical compliance of project’s outcomes/deliverables against applicable laws and regulations, providing suitable guidelines & recommendations.

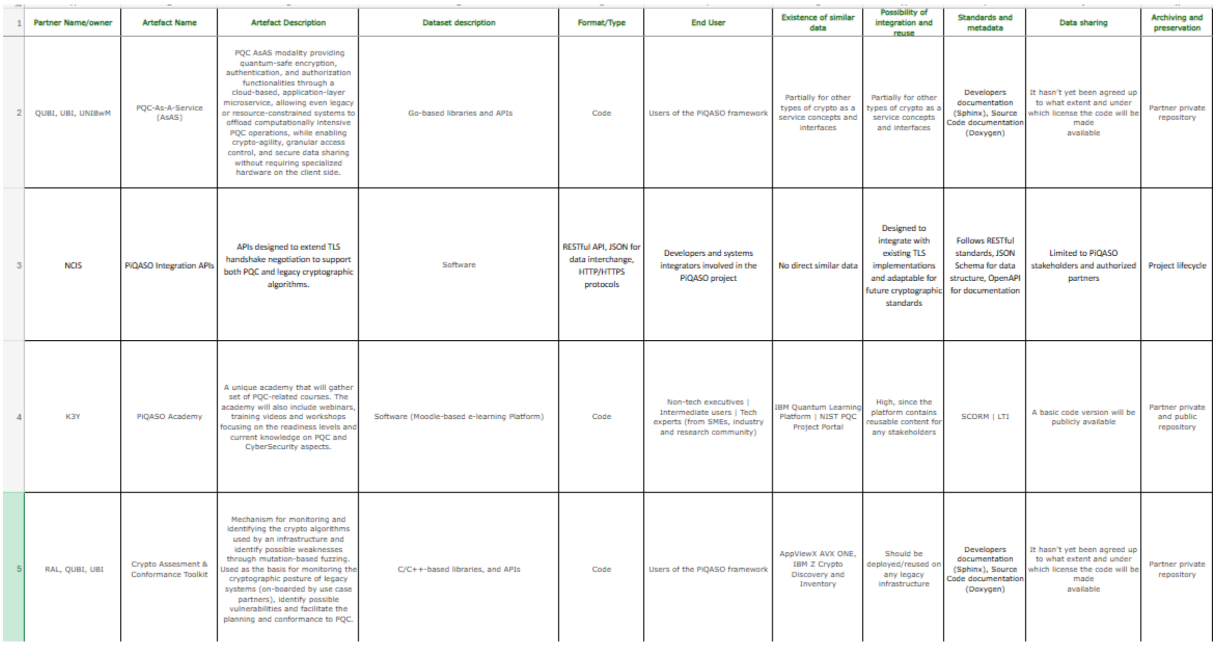
EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

9 Annexes

9.1 Annex I – PiQASO DMP Info Collector

Available here: DMP info collector-PiQASO.xlsx

Add print screen:



1	Partner Name/owner	Artefact Name	Artefact Description	Dataset description	Format/Type	End User	Existence of similar data	Possibility of integration and reuse	Standards and metadata	Data sharing	Archiving and preservation
2	QUBI, UBI, UNIBwM	PQC-As-A-Service (AsAS)	PQC AsAS modality providing quantum-safe encryption, authentication, and authorization functionalities through a cloud-based, application-layer microservice, allowing even legacy or resource-constrained systems to offload computationally intensive PQC operations, while enabling crypto-agility, granular access control, and secure data sharing without requiring specialized hardware on the client side.	Go-based libraries and APIs	Code	Users of the PiQASO framework	Partially for other types of crypto as a service concepts and interfaces	Partially for other types of crypto as a service concepts and interfaces	Developers documentation (Sphinx), Source Code documentation (Doxygen)	It hasn't yet been agreed up to what extent and under which license the code will be made available	Partner private repository
3	NCIS	PiQASO Integration APIs	APIs designed to extend TLS handshake negotiation to support both PQC and legacy cryptographic algorithms.	Software	RESTful API, JSON for data interchange, HTTP/HTTPS protocols	Developers and systems integrators involved in the PiQASO project	No direct similar data	Designed to integrate with existing TLS implementations and adaptable for future cryptographic standards	Follows RESTful standards, JSON Schema for data structure, OpenAPI for documentation	Limited to PiQASO stakeholders and authorized partners	Project lifecycle
4	K3Y	PiQASO Academy	A unique academy that will gather set of PQC-related courses. The academy will also include webinars, training videos and workshops focusing on the readiness levels and current knowledge on PQC and CyberSecurity aspects.	Software (Moodle-based e-learning Platform)	Code	Non-tech executives | Intermediate users | Tech experts (from SMEs, industry and research community)	IBM Quantum Learning Platform | NIST PQC Project Portal	High, since the platform contains reusable content for any stakeholders	SCORM | LTI	A basic code version will be publicly available	Partner private and public repository
5	RAL, QUBI, UBI	Crypto Assesment & Conformance Toolkit	Mechanism for monitoring and identifying the crypto algorithms used by an infrastructure and identify possible weaknesses through mutation-based fuzzing. Used as the basis for monitoring the cryptographic posture of legacy systems (on-boarded by use case partners), identify possible vulnerabilities and facilitate the planning and conformance to PQC.	C/C++-based libraries, and APIs	Code	Users of the PiQASO framework	AppViewX AVX ONE, IBM Z Crypto Discovery and Inventory	Should be deployed/reused on any legacy infrastructure	Developers documentation (Sphinx), Source Code documentation (Doxygen)	It hasn't yet been agreed up to what extent and under which license the code will be made available	Partner private repository

Keep in touch