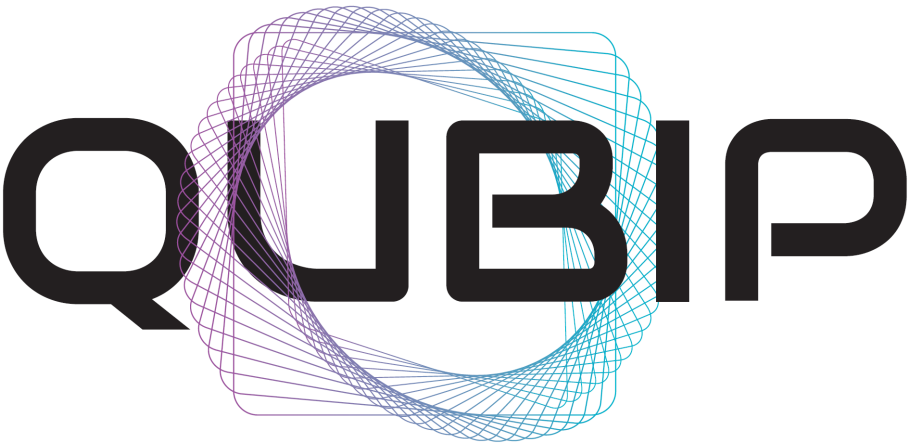
Horizon Europe




QUANTUM-ORIENTED UPDATE TO BROWSERS AND INFRASTRUCTURES FOR THE PQ TRANSITION (QUBIP)

# Policy Brief No. 1
# Regulating Quantum Computing

**Deliverable number: D4.7**

Version 1.0

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

**Project Acronym:** QUBIP
**Project Full Title:** Quantum-oriented Update to Browsers and Infrastructures for the PQ transition
**Call:** HORIZON-CL3-2022-CS-01
**Topic:** HORIZON-CL3-2022-CS-01-03
**Type of Action:** HORIZON-IA
**Grant Number:** 101119746
**Project URL:** https://www.qubip.eu
**Start date:** 1 September 2023
**Duration:** 36 months

| | | |
|---|---|---|
| Editor: | Alessandro Mantelero | – POLITO |
| Deliverable nature: | Report (R) | |
| Dissemination level: | Public (PU) | |
| Contractual Delivery Date: | 31 August 2024 | |
| Actual Delivery Date | 30 August 2024 | |
| Number of pages: | 22 | |
| Keywords: | Policy guidelines, regulatory framework, cybersecurity, post-quantum, cryptography | |
| Contributors: | David Arroyo<br>Marc Almeida<br>Izan Franco<br>Andrés Ruíz | – CSIC<br>– CSIC<br>– CSIC<br>– CSIC |
| Peer review: | Andrés del Álamo<br>Maria Chiara Molteni<br>Antonio Lioy | – CIB<br>– SECPAT<br>– POLITO |
| Approved by: | ALL partners | |

**Table 1:** Document revision history

| Issue Date | Version | Comments |
|---|---|---|
| 26/07/2024 | 0.1 | Initial ToC |
| 12/08/2024 | 0.2 | First draft version, for internal review |
| 19/08/2024 | 0.3 | Second version with contributors' additions |
| 30/08/2024 | 1.0 | Final version, for submission |

# Abstract

This document represents the Deliverable D4.7 of the Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition (QUBIP) project and contains the initial version of its Policy Brief, to be updated each year.

The changes introduced by quantum technologies and the associated technical issues are considered in this deliverable in terms of their impact on the regulatory framework. In this respect, D4.7 focuses on policy roadmapping from a regulatory perspective, leaving aside broader quantum technology industrial strategies adopted by governments. Taking into account the main pillars of technology regulation, i.e., safety, security and the protection of rights, an important element to be considered from a policy perspective is the limited reliability of quantum technologies with regard to their use in real-world applications with potential impacts on individuals and society.

This situation requires the adoption of policy strategies that combine both the precautionary principle and risk management methodologies. In addition, from an EU regulatory perspective, it is crucial to identify the weaknesses of the existing EU legal framework in dealing with a post-quantum scenario. In particular, several EU regulations set specific requirements in the field of data and cybersecurity that may be challenged by quantum technologies, making the current protection provided by the law inadequate.

In addressing this challenge, it is necessary to take into account the existing legal requirements, the possibility to implement quantum-resistant cryptography, and the quantum transition. In this context, this first Policy Brief provides a general overview of the regulatory challenges and offers initial guidance focusing on the policy and regulatory framework in general.

*Note to the reader: given its nature as a policy brief and its focus on the regulatory issues, this deliverable adopts the common standards used in the legal context and in the legal policy briefs with regard to the use of footnotes, citations, abbreviations, etc.*

# Contents

# List of Acronyms

| | |
|---|---|
| **AFNOR** | Association française de Normalisation [French Standardization Association] |
| **AI** | Artificial Intelligence |
| **ANSSI** | Agence Nationale de la Sécurité des Systèmes d'Information [French Cybersecurity Agency] |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik [German Federal Office for Information Security] |
| **CEN** | European Committee for Standardization |
| **CENELEC** | European Committee for Electrotechnical Standardization |
| **CRA** | Cyber Resilience Act |
| **DIN** | German Institute for Standardization |
| **EC** | European Commission |
| **ECCC** | European Cybersecurity Competence Center |
| **ENISA** | European Union Agency for Cybersecurity |
| **ETSI** | European Telecommunications Standards Institute |
| **EU** | European Union |
| **FGQT** | CEN/CENELEC Focus Group for Quantum Technologies |
| **FIPS** | Federal Information Processing Standards |
| **GDPR** | General Data Protection Regulation |
| **ICT** | Information and Communication Technologies |
| **IEC** | International Electrotechnical Commission |
| **IoT** | Internet of Things |
| **IPsec** | IP Security |
| **ISO** | International Organization for Standardization |
| **ITU** | International Telecommunication Union |
| **NCSA** | National Communications Security Agency |
| **NIST** | National Institute of Standards and Technology |
| **NLNCSA** | Netherlands National Communications Security Agency |
| **NSS** | Network Security Services |
| **PQ/T** | Post-Quantum/Traditional |
| **PQC** | Post-Quantum Cryptography |
| **QCI** | Quantum Communication Infrastructure |
| **QCT** | Quantum Computing Technology |
| **QKD** | Quantum Key Distribution |
| **QT** | Quantum Technologies |
| **QUBIP** | Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition |
| **TRL** | Technology Readiness Level |
| **UNE** | Spanish Association for Standardization |
| **UNI** | Italian Standardization Body |

# 1 Introduction

In April 2024, the European Commission published its recommendation on a *Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography* (C(2024) 2393 final). The Commission Recommendation on Post-Quantum Cryptography (PQC) builds on the policy objectives set out in the EU's Cybersecurity Strategy for the Digital Decade (JOIN/2020/18 final), for improving the end-to-end security and resilience of the Union's digital infrastructures and services for public administrations and other critical infrastructures; it serves the objectives of the Digital Single Market, and of the Joint Communication on European Economic Security Strategy 10919/23.[1]

The *Post-Quantum Cryptography Coordinated Implementation Roadmap* should promote interoperability between countries, allowing systems and services to function seamlessly across borders by clearly indicating actions to be implemented by EU Member States to guarantee an effective transition and adoption of PQC algorithms. With regards to PQC algorithms, National Institute of Standards and Technology (NIST) has published in August 2024 three Federal Information Processing Standards (FIPS) for PQC, which are called FIPS-203, -204, and -205. The new FIPS standards are designed to protect information exchanged across public networks and digital signatures used for identity authentication via hybrid schemes that may combine PQC with existing cryptographic approaches or with Quantum Key Distribution (QKD).

In January 2024, the German Federal Office for Information Security (BSI) in collaboration with European partner agencies from France (ANSSI), the Netherlands (NLNCSA), and Sweden (Swedish NCSA), published a position paper[2] on the topic of QKD. The report analysed the limitations and challenges of this technology advising its adoption only in some niche use cases as it is not yet sufficiently mature from a security perspective to be adopted at scale and requires further work to advance protocol standards and other QKD-related standards, on security proofs, and on evaluation methodologies.

On the contrary, PQC is considered a mature technology that can be deployed in classical communication infrastructures, as it can be implemented on classical hardware. Considering the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the authors of the position paper suggest to prioritise the migration to PQC in hybrid solutions with traditional symmetric keying or classically secure public-key cryptography.

Similarly, the US Government considers the transition to PQC a priority and has established a strict roadmap for implementing NIST standards in web browsers, servers, cloud services, and operating systems by 2033. This transition is shaking the foundations of the entire digital ecosystem and it is creating the major challenge of adopting the correct organisational and technical measures to guarantee continuity of services while going through the transition. The European Commission recommends[3] EU Member States and the Union to cooperate actively with their international strategic partners in the development of international standards in PQC with a view to ensuring interoperability of communications going forward. European Standards Bodies (CEN, CENELEC and ETSI)[4] contribute to support European legislation and political priorities by providing harmonised standards for the common market through the cooperation with national standardisation bodies (e.g., DIN in Germany, UNE in Spain, AFNOR in France, UNI in Italy), international standardisation bodies (e.g., IEC, ISO, ITU) and institutions in other countries such as NIST in the US.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 2 Quantum technologies made in Europe

## 2.1 Towards European Quantum Computing

The need for developing and implementing PQC comes from the risk of facing a malevolent agent owning a quantum computer, achieving quantum supremacy, and so able to break the algorithms underlying the encryption keys that safeguard our data and the Internet's infrastructure (ETSI 2015)[5]. A comprehensive overview of the capabilities of quantum computing as a potential cybersecurity threat has been included in QUBIP deliverable D1.1 "Expected capabilities of Quantum Computers". In this section we briefly revise actions taken by the EU to achieve a fully-fledged European quantum ecosystem that builds on its tradition of excellence in quantum research.

Following the Quantum Manifesto in 2016, the Quantum Technologies Flagship was launched in 2018 to foster the collaboration between research institutions, industry players, and public funders. The EU Digital Decade Strategy set the ambitious objective for Europe of having its first supercomputer with quantum acceleration by 2025 and being at the cutting edge of quantum capabilities by 2030. In addition, the European Chips Act includes measures to foster the low-cost, high-volume manufacturing of quantum chips in the EU, so that they can power a whole range of innovative quantum devices.

Since June 2019, all 27 EU Member States have signed the EuroQCI Declaration leading to the creation of a Quantum Communication Infrastructure (QCI) across the EU. The Commission is investing in pan-European quantum sensing infrastructures that will link these sensors and harness their potential, including a network of quantum gravimeters, both fixed and mounted on moving carriers like drones or ships, that will monitor underground and underwater resources and volcanic activity, carry out Earth observation tasks, and more. This network will be connected to a planned European space gravimetry infrastructure, enabling even more precise measurements to be made with the support of space-based technologies.

## 2.2 The contribution of QUBIP

QUBIP implements and validates at TRL6 public-key PQC in three use cases, which are IoT-based Digital Manufacturing (PQ/T for resource-constrained devices and embedded systems) and Software Networks Environments for Telcos (Quantum safe key exchange and IPsec) and Internet Browsing (PQC integration into OpenSSL and NSS). Lessons learnt from these three practical exercises will be summarised by LINKS in deliverable D3.3 'Migration Playbook' at the end of the project. These lessons will include any technical, economic, and legal barrier encountered and all best practices adopted to overcome them and create a structured process that can be easily replicated by industrial stakeholders.

QUBIP explores changes brought along with the advent and implementation of quantum computing, quantum-resistant cryptography and QKD. As it is crucial to deal with the risk that existing data protection and cybersecurity legislation may be partly useless rather pointless in the face of Quantum Computing. Two main elements must be considered: (*i*) the consequences of quantum computing on the existing obligations in the field of data and cybersecurity; (*ii*) the fact that changes in the existing legislation may be difficult to achieve and not easy to implement in a short timeframe.

Given the length of the legislative process, and the little room for further changes during the current wave of new and ongoing regulation in the digital sector, it is therefore necessary to define a strategy to cope with the principles set by various pieces of EU legislation in terms of strong data security by updating the technical requirements that pre-quantum provisions have established. This action to create a bridge between

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

the pre-quantum legal framework and the future quantum framework to come, including EU strategies and research agendas on Quantum critical technologies. This policy brief is an attempt to contribute to the debate about the best regulatory pathways toward the creation of quantum technologies aligned with European values, norms and principles.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 3 European regulatory and standardisation efforts around quantum technologies

Following the progress achieved under the previous strategies, EU's Cybersecurity Strategy contains concrete proposals for deploying three principal instruments – regulatory, investment, and policy instruments – to address three areas of EU action: (1) resilience, technological sovereignty, and leadership, (2) building operational capacity to prevent, deter, and respond, and (3) advancing a global and open cyberspace. Furthermore, cybersecurity must be integrated into all digital investments, particularly key technologies like Artificial Intelligence (AI), encryption, and quantum computing, using incentives, obligations, and benchmarks.

The EU Cybersecurity Act (Regulation EU 2019/881) established the European Cybersecurity Certification Framework in order to improve the conditions for the functioning of the internal market. As laid down in the mandate provided by the EU Cybersecurity Act, the European Union Agency for Cybersecurity (ENISA) can be requested to prepare candidate EU cybersecurity certification schemes. All schemes must contain references to the international, European or national standards applied in the evaluation of ICT products, ICT services and ICT processes. There is a close linkage between the tasks assigned by ENISA to that purpose, and the Rolling Plan for ICT Standardisation. The EU as other national regulators are placing increasingly demanding Cyber Security assurance and information threat sharing requirements on manufacturers and operators of ICT products and services. While many of these initial regulations are effectively optional, second generation regulations such as the EU Cyber Resilience Act (CRA) will place mandatory requirements on manufacturers and service providers.

The NIS2 Directive (Directive (EU) 2022/2555) lays down cybersecurity risk-management measures and reporting obligations for entities operating in critical and highly critical sectors to achieve a high common level of cybersecurity across the EU. In order to promote a convergent implementation of the cybersecurity risk management measures across the EU, Member States should encourage the use of European or international standards and technical specifications relevant to the security of network and information systems, without imposing or discriminating in favour of the use of a particular type of technology. The NIS2 Directive amends the eIDAS Regulation and includes the requirements concerning cybersecurity risk-management and incident reporting for the trust service providers.

In February 2024, the Commission adopted the first-ever European cybersecurity certification scheme, based on the tried and tested Common Criteria (ISO/IEC 15408) and Common Evaluation Methodology (ISO/IEC 18045). The scheme offers a Union-wide set of rules and procedures on how to certify ICT products in their lifecycle and thus make them more trustworthy for users. The voluntary scheme will complement the Cyber Resilience Act that introduces binding cybersecurity requirements for all hardware and software products in the EU. The European Digital Identity Wallets is another area where European cybersecurity certification schemes are envisaged linked to legislative developments. Furthermore, areas for future reflection regarding cybersecurity certification include Industrial Automation and Control Systems and Security Lifecycle Development building on the CRA requirements as well as cryptographic mechanisms. The implementation of the CRA, the AI Act and the Digital Identity Regulation (the revised eIDAS Regulation) may require further standardisation activities, including in the area of cybersecurity.

Commission Recommendation (EU) C(2024) 2393 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to PQC represents a stepping stone for EU policy in the field of digital technologies, in line with the EU Security Union Strategy and the EU Cybersecurity Strategy, which both highlight encryption as a key technology for achieving resilience, technological sovereignty, and for building operational capacity to prevent cyberattacks.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

The Communication on *ICT Standardisation Priorities for the Digital Single Market* (COM/2016/0176 final)[6] has identified the following priority areas: 5G communications, cloud computing, the Internet of Things (IoT), (big) data technologies and cybersecurity. Quantum technologies can revolutionise all these areas, which represent the essential technology building blocks of the Digital Single Market. Transparent standards and specifications for the definition and verification of cybersecurity requirements form the very foundation of the "cybersecurity-by-design-and-default" proposition the European Union aims for, such as the continuous monitoring of the threat landscape for the purpose of aftermarket improvements to the sold ICT and the support with threat intelligence to remain resilient in the next wave of cyberattacks.

As clearly stated in the *Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*, the sub-group on Post-Quantum Cryptography shall exchange information with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges. During the sixth ministerial meeting[7] of the EU-US Trade and Technology Council and Cyber Dialogue, the European Union and the United States established a Quantum Task Force to foster their mutual cooperation on Quantum Technologies (QT) research. Since June 2020, the CEN/CENELEC Focus Group for Quantum Technologies (FGQT) supports the plans of the Commission to identify standardisation needs and opportunities for QT, while also promoting liaison with relevant existing CEN/CENELEC and ISO Technical Committees. As the Quantum Flagship, the CEN/CENELEC FGQT roadmap is structured around the four major areas of QT: communication, computing, simulation, sensing, and metrology.

As outlined in report D4.4 "Standardisation plan and activities" several standardisation activities in QT are ongoing worldwide, with overlaps in some areas and neglect in others. Selected members of the QUBIP consortium are participating in the activities of CEN-CLC/JTC 13 'Cybersecurity and Data Protection' and CEN/CLC/JTC 22 WG4. In the case of CEN-CLC/JTC 13, it has been established a dedicated Special Working Group on Cyber Resilience Act (CEN/CLC/JTC 13/WG 9) to continue work already carried out in the Special Working Group RED Standardization Request (CEN/CLC/JTC 13/WG 8).

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 4 Why quantum computing is a regulatory issue

The paradigm shift towards Quantum Computing Technology (QCT)[8] involves a number of important technological challenges in computational techniques and raises complex issues from a computer science perspective. However, from a policy and regulatory perspective, the viewpoint is different[9]. The technical elements are considered in a functional way, in relation to the interests protected by the law. The latter, in terms of technology regulation, can be grouped into the triad of safety, security and rights protection.

The changes introduced by QCTs and the technical issues involved therefore need to be considered in terms of their impact on the regulatory framework and society. In this regard, according to the QUBIP project description, D4.7 focuses on policy roadmapping from a regulatory perspective, leaving aside broader QCTs industrial strategies adopted by governments[10].

From this perspective, the first elements to consider are the **effectiveness of the QCTs solutions** under development and their **transformative consequences for individuals and society**. Regarding effectiveness, this is the necessary starting point for all technology assessment from a policy perspective. In terms of policy and standard setting, the current situation of QCTs replicates the well-known Collingridge dilemma[11] on the information problem about the potential impacts of new technology development. On the one hand, when the technology is still under development and its potential applications are not fully defined, as in the case of QCTs, the adoption of regulatory guidelines can be critical because it is difficult to predict all possible consequences. As a result, early regulation could frame some issues in the wrong way and have a negative impact on technology development. On the other hand, if regulation comes too late, it can be difficult to change established practices and standards set by dominant players.

With regard to QCTs, although the idea of building computers based on quantum mechanics was proposed in the early 1980s, concrete implementations had not been achieved by the end of the millennium[12]. Although recent developments in this field have moved QCTs from research laboratories to industry, it is worth noting that this technology is not sufficiently mature and QCTs present significant margins of error. This is an important element to consider from a policy perspective, as a limited reliability of the QCTs results hinders its full use in real-world applications with potential impact on individuals and society[13].

Given that the regulation of technology, as noted above, is about safety, security and the protection of rights, dealing with a technology characterised by errors is both an inherent limitation of that technology and a risk From a policy perspective, this situation is usually addressed by combining the **precautionary principle** and **risk assessment & management methodologies**. The precautionary principle has its origins in the environmental legislation of the last decades of the 20th century and is also enshrined in the Treaty on the Functioning of the European Union and in the national legislation of some Member States[14]. This principle deals with scientific uncertainty and addresses the case where uncertainty[15] makes it impossible to conduct a concrete risk assessment of a given technology. On the other hand, where the level of uncertainty is not so high, the risk assessment process is a valuable tool for managing the risks stemming from technology applications[16].

Based on this framework, where QCTs show immaturity and a significant error rate, a precautionary approach suggests that QCTs should not be used in applications that impact on individuals and society. This does not stop research on QCTs, on the contrary research development contributes to better define future operational scenarios where the level of maturity of QCTs can be fully achieved. Once this maturity is achieved and potential impacts can be properly assessed, it will be possible to move from a precautionary approach to a risk-based approach adopting appropriate risk management procedures in real-life implementation of quantum technologies.

In view of these considerations, in terms of policy assumptions, the exclusion of an immediate use of

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

QCTs for societal purposes (for both technical reasons and the precautionary principle) does not preclude the relevance of policy issues in considering **possible future uses and how to properly address the associated challenges**. In this respect, we need to consider, for example, how to deal with the expectation that QCTs will be able to break the most secure cryptographic algorithms that exist today within 15 to 30 years[17]. In addition, the factors that discourage the immediate use of QCTs in society, from a responsible innovation perspective[18], do not prevent **this technology from being used for malicious purposes by criminal actors**. The latter scenario represents a serious threat, notwithstanding the fact that the inherent limitations of quantum technology may hinder the full achievement of the malicious purpose in all the cases.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 5 The EU regulatory perspective and the QUBIP policy briefs

Based on the considerations on QCT expressed in the previous section and with a view to the potential impact of QCT, it is crucial to identify the **weaknesses of the existing EU legal framework** in dealing with a post-quantum scenario. In particular, several EU regulations set specific requirements in the field of data protection and cybersecurity that can be challenged by QCT making the current protection provided by the law inadequate[19].

As cybersecurity is the main issue in facing the challenges of QCTs in the case of malicious use of this technology, QUBIP aims to develop effective solutions for quantum cryptography that can properly respond to this challenge and create a secure QCT environment[20]. In this context, it is possible to develop quantum-resistant cryptographic solutions based on mathematical problems that are resistant to attack by quantum computers, without having a quantum computer for it[21]. These algorithms can already be used today, and it is possible to start the transition immediately, which is necessary for the reasons discussed in the previous section. This entails a **transition phase** requiring standard setting and implementation in a variety of sectors characterised by different issues[22].

From a policy perspective and at EU level, taking into account the time needed for the general implementation of quantum cryptography and the progressive nature of the development of QCTs in all the sectors, **it is therefore necessary to consider three elements: (*i*) the existing legal requirements; (*ii*) the possibility to implement quantum-resistant cryptography; (*iii*) the quantum transition**.

While this first Policy Brief provides a general overview of the challenges related to QCT, the subsequent policy briefs will carry out a mapping and risk identification exercise, followed by a roadmapping exercise in terms of regulation and some sector-specific analyses.

In order to provide final guidance to policy makers and regulators at the end of the project, in line with the task assigned, a progressive approach has been adopted, rather than considering the regulatory issues as a 'final check' exercise. In this respect, three deliverables are planned, one at the end of each year. This will allow policy analysis to progress hand in hand with the project development and the ongoing regulatory debate at the EU level.

The mapping of the existing regulatory framework and the development of policy guidance will require **a specific focus on the 'transition phase'**. Taking a conservative approach due to standard-setting, regulatory and market constraints, it is important to consider the risks associated with this phase, in which quantum-resistant solutions will not be fully implemented in all the sectors (due to their nature) or by all the actors (due to the different responses). As a result, there will be entities or objects that are vulnerable to quantum-based hacking.

It is therefore crucial to perform a **risk analysis** that distinguishes between the following situations: (*i*) high-risk contexts, where quantum attacks are expected and the systems/devices, as defined by legal requirements, will not be quantum resistant; (*ii*) medium risk contexts, where vulnerabilities exist but quantum resistant solutions can be implemented within the existing legal framework; (*iii*) low risk contexts, where there are no potential targets for quantum attacks and no specific legal requirements need to be defined

In this respect, it is worth emphasising that the transition is not just a matter of moving from one cryptographic standard to another, in a simple on/off situation. The time factor therefore has a significant impact on the transition phase.

For example, some data breaches may not be considered high risk under the GDPR, due to the use of cryptography, but stolen datasets may become vulnerable in future years due to the use of quantum hacking[23]. This is a risk that is not currently covered in the assessment of the impact of data breaches and

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

can be mitigated by appropriate policies in terms of awareness raising and the remedies to be adopted following a data breach.

In other cases, the nature of the system and the long lifecycle of the product may make ex post security updates with the introduction of quantum-resistant solutions difficult (e.g., some IoT devices cannot be upgraded to post-quantum security protection).

A second important aspect relates to the way in which the technical requirements are defined in the various pieces of relevant legislation. In this respect, high-risk situations are those where the legal provisions are not sufficiently broad and open to include quantum cryptography among the protection measures provided by the law, namely when the law refers to specific standards or technical requirements that are not quantum-based and vulnerable to quantum-based attacks. For this reason, an analysis of the existing relevant legal requirements will be carried out in the next policy brief.

It is important to note that from a regulatory perspective, risk assessment and vulnerabilities are examined by looking at existing legal requirements, rather than from a bottom-up industry perspective. Thus, the level of risk is based on what technical protection is required by law provisions and how this may be challenged by quantum-based hacking. This may include both general cross-industry regulations (e.g., the GDPR, the AI Act, etc.) and sector-specific legal instruments, such as the PSD2 Directive. In addition, the legal analysis must also identify the existence of **industry sectors that do not have specific regulation, but need it** to meet the challenges posed by quantum computing.

Finally, the approach adopted focuses on the existing legal framework rather than on general policy principles, such as transparency and accountability[24], which can be interpreted in many different ways and are to a large extent already part of EU regulation of the digital society.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 6 Looking at the regulatory dimension in policy drafting

Based on the previous considerations, initial guidelines can be outlined focusing on the policy and regulatory framework in general, as a starting general approach in view of the sector-specific recommendations that will be provided in the next Policy Brief with regard to the specific elements of the EU regulation.

1. In view of the relationship between the precautionary principle and the risk-based approach adopted by the EU in the field of technology and, in particular, in the regulation of the digital society (see, e.g., the GDPR and the AI Act), **further research needs to be promoted** (*i*) **to define the best technical solutions** to overcome the existing limitations of QCT and the associated negative consequences for individuals and society, and (*ii*) **to better understand the risk and associated impacts of QCT**, as well as to carry out appropriate technology and risk assessments[25].
2. Research in this field is also crucial to move from the technical readiness and feasibility of quantum-resistant solutions, such as post-quantum cryptography, to the technical standardisation of these solutions. **The link between the research results and the management of the transition phase needs to be fostered** and kept open to the **active participation of relevant stakeholders and rights holders**.
3. From a legal perspective, it is important to consider the intersection of quantum technologies and cybersecurity from the perspective of the digital ecosystem created by the regulation, not only considering the technical availability of solutions to counter potential threats, but also **ensuring the alignment of legal and technical requirements and standards**.
4. Promote regulatory **coordination at EU level with regard to the different pieces of legislation regulating the digital society and, in particular, cybersecurity**. This should be done by taking into account the whole regulatory environment, **looking at the interplay between EU and national provisions**, where the interaction with national practices and rules may weaken the robustness of the EU framework in terms of legal obligations, even more so during the transition period.
5. Encourage the **active involvement of the various EU policy bodies**, with a focus on cybersecurity and data protection.
6. Encourage **risk awareness initiatives**, by promoting awareness campaigns and QCT skills among both the technical and legal communities of experts[26], including through the collection of best practices in quantum technology applications for the quantum transition.
7. Focus on the **critical infrastructure** from a technology assessment, non-legal, perspective.
8. Promote EU governance based on the **risk-based approach with the introduction of participatory elements**, involving the research community.
9. Facilitate **policy coordination between the EU, Member States, national cybersecurity agencies, the European Cybersecurity Competence Center (ECCC), and the ENISA** to set technology priorities and identify relevant use cases for quantum-secure technologies. This is particularly important during the transition period when some Member States may individually implement the use of post-quantum encryption and other quantum-based cybersecurity solutions.
10. Facilitate **technical coordination at the EU and international level**, to address research gaps in quantum-secure technologies and to harmonise the approach to QCT development and technology standards.
11. **Assess the geopolitical implications of quantum technologies**[27] and related gaps in the development of a secure and trustworthy environment, including by **addressing the potential risk of widening existing digital divides and related inequalities** affecting some digital societies or parts thereof.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

## Notes

[1]European Commission. 2023. Joint communication on “European Economic Security Strategy”.

[2]BSI. 2024. Position Paper on Quantum Key Distribution.

[3]European Commission. 2024. Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography.

[4]European standards. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. https://single-market-economy.ec.europa.eu/single-market/european-standards_en

[5]ETSI. 2015. Quantum Safe Cryptography and Security – An introduction, benefits, enablers and challenges.

[6]European Commission. 2016. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ICT Standardisation Priorities for the Digital Single Market. COM/2016/0176 final.

[7]European Commission. 2024. Joint Statement EU-US Trade and Technology Council of 4-5 April 2024 in Leuven, Belgium.

[8]QCTs exploit the possibilities offered by the latest technology to directly manipulate individual quantum systems and use quantum phenomena to enable a new class of technologies based on quantum mechanics.

[9]See also Hoofnagle, Chris Jay and Garfinkel, L. Simson. 2022. Law and Policy for the Quantum Age (Cambridge: Cambridge University Press).

[10]See, e.g., QuantERA. 2023. Quantum Technologies Public Policies in Europe. All websites and materials available online were accessed between February and August 2024.

[11]The Collingridge dilemma, also known as the ‘dilemma of control’ can be summarised as follows based on its author’s words: “attempting to control a technology is difficult [...] because during its early stages, when it can be controlled, not enough can be known about its harmful social consequences to warrant controlling its development; but by the time these consequences are apparent, control has become costly and slow”. See Collingridge, David. 1980. The Social Control of Technology (London-New York: Frances Pinter).

[12]See also Nature Reviews Physics 2022 “40 years of quantum computing”.

[13]Quantum technologies for computation suffer from significant limitations in terms of the quality of their output, while better performance has been achieved in some areas (e.g., quantum key distribution, clock synchronisation, random number generation) and commercial applications are available in sensing and metrology. See also EUROPOL 2023 and RHC 2024.

[14]See also European Parliament. 2015. The Precautionary principle Definitions, applications and Governance.

[15]Commission of the European Communities. 2000. Communication from the Commission on the precautionary principle, COM(2000) 1 final, 8-16; Hansson, Sven Ove. 2020. How Extreme Is the Precautionary Principle? 14 NanoEthics 245–257. Only few contributions in law literature consider the application of the precautionary approach in the field of data protection, see Costa, Luiz. 2012. Privacy and the precautionary principle. 28(1) Computer Law & Security Review 14–24; Gonçalves, Maria Eduarda. 2017. The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. 26(2) Inform. Comm. Tech. Law 90-115; Pieters, Wolter. 2011. Security and Privacy in the Clouds: A Bird’s Eye View. In: Gutwirth Serge et al. (eds) Computers, Privacy and Data Protection: An Element of Choice (Springer: Dordrecht), 445-457. On the precautionary approach in data protection, see also Narayanan, Arvind, Joanna Huey, and Edward W. Felten. 2016. A Precautionary Approach to Big Data Privacy. In: Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds). 2016. Data Protection on the Move (Springer: Dordrecht) 357-385; Raab, Charles and Wright, David. 2012. Surveillance: Extending the Limits of Privacy Impact Assessment. In: Wright, David and De Hert, Paul (eds). Privacy Impact Assessment (Springer: Dordrecht) 363-383, 364.

[16]The relationship between risk assessment and the precautionary principle is rather complicated and cannot be reduced to a strict alterative. Indeed, if a precautionary approach suggests that a technology should not be used in a given social context, this does not necessarily mean that its development should be halted. On the contrary, where there is no incompatibility with human rights, the technology can be developed further to reach a sufficient level of maturity that shows awareness of the related risks and the effective solutions.

[17]See Michele Mosca and Marco Piani. 2022. Quantum Threat Timeline Report 2022. Global Risk Institute in Financial Services, 17-26.

[18]European Commission, Directorate-General for Research and Innovation. 2014. Responsible research and innovation: Europe’s ability to respond to societal challenges. See also Griesdoorn, Ferdinand, Kroesen, Maarten, Vermaas, Pieter and van de Poel, Ibo. 2023. The presence of Responsible Research and Innovation in the perspectives of Dutch policy officers regarding innovation with quantum technology. 16 Journal of Responsible Technology 100071.

[19]For example, the use of QCT in the field of imagining can lead to the production of devices that can potentially see through obfuscating conditions, such as fog, smoke, or even in complete darkness, raising concerns in terms of privacy and data protection to be addressed by specific guidelines, rather than new specific legal provisions. See Regulatory Horizons Council (2023), p. 39.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

[20]"Around two thirds of the 90 billion cryptographic devices use public key cryptography, and of those, 95-99% rely on the computational hardness of factoring products of large prime numbers and the discrete log problem, both of which quantum computers can solve efficiently". See also Rodríguez, Andrea G. 2023. Governing the Transition to Post-Quantum Cryptography.

[21]See NIST (2023). New Encryption Standards Protect Against Post-Quantum Attacks.

[22]See, for example, EUROPOL (2023), on the QCT impact on the law enforcement sector. See also Regulatory Horizons Council (2023), 8, 28-29; Mosca and Piani (2022).

[23]See also EUROPOL (2023), 11.

[24]See, e.g., UK Government (2023). Policy paper: National quantum strategy. Department for Science, Innovation and Technology; World Economic Forum. 2022. Quantum Computing Governance Principles; Mauritz Kop et al. 2023. 10 Principles for Responsible Quantum Innovation; Department for Science, Innovation and Technology. 2023. A pro-innovation approach to AI regulation.

[25]See EUROPOL (2023), 8. It is worth noting that technology assessment concerns a technology in general, whereas risk assessment concerns the application of that technology in a specific context. See also Rasmus Øjvind Nielsen et al. 2015. Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and selected other countries. Deliverable 1.1 ("technology assessment (TA) is a form of impact assessment that is specifically developed to assess impacts of a new technology. TA investigates the potential and actual effects of new technologies on industry, the environment and society, evaluates such effects and develops instruments to steer technology development in more desirable directions. TA makes such assessments on the basis of known or potential applications of the technology. It pays special attention to consequences that are unintended, indirect or delayed."). See also Grunwald, Armir. 2020. The Objects of Technology Assessment. Hermeneutic Extension of Consequentialist Reasoning. 7(1) Journal of Responsible Innovation 96–112; Grunwald, Armin. 2018. Technology Assessment in Practice and Theory (Routledge: Milton); Grunwald, Armin. 2009. Technology Assessment: Concepts and Methods. In Meijers, Anthonie W.M. (ed) Philosophy of Technology and Engineering Sciences. Handbook of the Philosophy of Science, vol. 9 (North Holland: Amsterdam), 1103-1146.

[26]See also EUROPOL (2023), 7; Regulatory Horizons Council (2023), 26-27.

[27]Mosca and Piani (2022), pp. 37-38.

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

# 7 Bibliography


Bova, Francesco, Avi Goldfarb, and Roger G. Melko. 2021. Commercial applications of quantum computing. 8(1):2 EPJ quantum technology. DOI 10.1140/epjqt/s40507-021-00091-1

BSI. 2024. Position Paper on Quantum Key Distribution. 26/01/2024. Federal Office for Information Security. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

CEN-CENELEC. 2023. Standardization Roadmap on Quantum Technologies, https://www.standict.eu/publications/standardization-roadmap-quantum-technologies-cen-cenelec-focus-group-quantum

Collingridge, David. 1980. The Social Control of Technology (London-New York: Frances Pinter).

Commission of the European Communities. 2000. Communication from the Communication from the Commission on the precautionary principle, COM(2000) 1 final.

Costa, Luiz. 2012. Privacy and the precautionary principle. 28(1) Computer Law & Security Review 14–24.

European Commission. 2024. Joint Statement EU-US Trade and Technology Council of 4-5 April 2024 in Leuven, Belgium. https://ec.europa.eu/commission/presscorner/detail/en/statement_24_1828

European Commission. 2016. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ICT Standardisation Priorities for the Digital Single Market. COM/2016/0176 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0176

European Commission. 2023. Joint communication to the European Parliament, the European Council and the Council on “European Economic Security Strategy”. JOIN/2023/20 final. 20/06/2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020

European Commission. 2024. Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. https://ec.europa.eu/newsroom/dae/redirection/document/104249

ETSI. 2015. Quantum Safe Cryptography and Security – An introduction, benefits, enablers and challenges.

European Commission, Directorate-General for Research and Innovation. 2014. Responsible research and innovation: Europe’s ability to respond to societal challenges. https://op.europa.eu/en/publication-detail/-/publication/2be36f74-b490-409e-bb60-12fd438100fe

European Parliament. 2015. The Precautionary principle Definitions, applications and Governance, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/573876/EPRS_IDA(2015)573876_EN.pdf

EUROPOL. 2023. The Second Quantum Revolution: The impact of quantum computing and quantum technologies on law enforcement, https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement

Flöther, Frederik F. 2023. The state of quantum computing applications in health and medicine. 1 Research Directions: Quantum Technologies. DOI 10.1017/qut.2023.4

Gonçalves, Maria Eduarda. 2017. The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. 26(2) Inform. Comm. Tech. Law 90-115.

Griesdoorn, Ferdinand, Maarten Kroesen, Pieter Vermaas, and Ibo van de Poel. 2023. The presence of Responsible Research and Innovation in the perspectives of Dutch policy officers regard-


*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

ing innovation with quantum technology. 16 Journal of Responsible Technology 100071. DOI 10.1016/j.jrt.2023.100071

Grunwald, Armin. 2009. Technology Assessment: Concepts and Methods. In Anthonie W.M. Meijers (ed) Philosophy of Technology and Engineering Sciences. Handbook of the Philosophy of Science, vol. 9 (North Holland: Amsterdam), 1103-1146.

Grunwald, Armin. 2018. Technology Assessment in Practice and Theory (Routledge: Milton)

Grunwald, Armir. 2020. The Objects of Technology Assessment. Hermeneutic Extension of Consequentialist Reasoning. 7(1) Journal of Responsible Innovation 96–112, DOI 10.1080/23299460.2019.1647086

Gutwirth S, Leenes R, De Hert P (eds). 2016. Data Protection on the Move. Springer, Dordrecht, 357-385.

Gutwirth, Serge, Ronald Leenes, and Paul De Hert (eds). 2016. Data Protection on the Move (Springer: Dordrecht) 357-385.

Gutwirth, Serge, Yves Poullet, Paul De Hert, and Ronald Leenes (eds). Computers, Privacy and Data Protection: An Element of Choice (Springer: Dordrecht).

Hansson, Sven Ove. 2020. How Extreme Is the Precautionary Principle? 14 NanoEthics 245–257.

Hoofnagle, Chris Jay and Simson L. Garfinkel. 2022. Law and Policy for the Quantum Age (Cambridge: Cambridge University Press).

Kop, Mauritz et al. 2023. Towards Responsible Quantum Technology. Harvard Berkman Klein Center for Internet & Society Research Publication Series #2023-1. DOI 10.2139/ssrn.4393248

Majot, Andy and Roman Yampolskiy. 2015. Global catastrophic risk and security implications of quantum computers. 72 Futures 17-26.

Mauritz Kop et al. 2023. 10 Principles for Responsible Quantum Innovation, https://law.stanford.edu/publications/10-principles-for-responsible-quantum-innovation/

Mosca, Michele and Marco Piani. 2022. Quantum Threat Timeline Report 2022. Global Risk Institute in Financial Services, 17-26.

Nature. 2022. 40 years of quantum computing, https://www.nature.com/collections/djhfiebiig

NIST. 2023. New Encryption Standards Protect Against Post-Quantum Attacks. 02/17/2023. https://govciomedia.com/new-encryption-standards-protect-against-post-quantum-attacks/

Possati, Luca M. 2023. Ethics of Quantum Computing: An Outline. 36(3) Philosophy & Technology: 48. DOI 10.1007/s13347-023-00651-6

QuantERA. 2023. Quantum Technologies Public Policies in Europe, https://quantera.eu/quantum-technologies-public-policies-report-2023/

Rasmus Øjvind Nielsen et al. 2015. Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and selected other countries. Deliverable 1.1, https://satoriproject.eu/media/D1.1_Ethical-assessment-of-RI_a-comparative-analysis.pdf

Regulatory Horizons Council (RHC). 2024. Regulating Quantum Technology Applications, 37-49, https://www.gov.uk/government/publications/regulatory-horizons-council-regulating-quantum-technology-applications

Rodríguez, Andrea G. 2023. Governing the Transition to Post-Quantum Cryptography. https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf

UK Government. 2023. Policy paper: National quantum strategy. Department for Science, Innovation and Technology. 14 December 2023. https://www.gov.uk/government/publications/national-quantum-strategy

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*

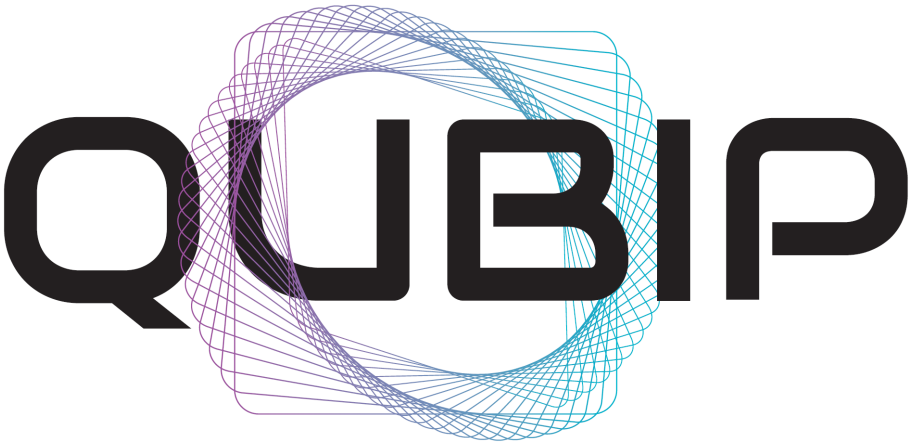
UK Government, Department for Science, Innovation and Technology. 2023. A pro-innovation approach to AI regulation. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

UK Government, Department for Science, Innovation and Technology. 2023. National quantum strategy. https://www.gov.uk/government/publications/national-quantum-strategy

World Economic Forum. 2022. Quantum Computing Governance Principles, https://www.weforum.org/reports/quantum-computing-governance-principles/

Wright, David and Paul De Hert (eds). 2012. Privacy Impact Assessment (Springer: Dordrecht).

*This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].*



Quantum-oriented Update to Browsers and Infrastructures for the PQ transition (QUBIP)

https://www.qubip.eu

# D4.7 – Policy Brief No. 1 Regulating Quantum Computing

Version 1.0

Horizon Europe