KPMG

# Quantum computing and data privacy: What your privacy team needs to know now

# Quantum computing: Opportunities are coming

Quantum computing is set to revolutionize industries—accelerating drug discovery in healthcare, transforming risk management and fraud detection in finance, and unlocking new frontiers in artificial intelligence and logistics. Across sectors, it will provide a significant competitive edge and usher in the next wave of digital transformation. Quantum computing isn't just a topic for your cybersecurity team—it directly affects how your organization protects personal data. Major enterprise platforms encrypt data using classical algorithms (Rivest-Shamir-Adleman [RSA], elliptic curve cryptography). These are the same algorithms quantum computers are designed to break. That means:

- Data flowing through your enterprise platforms today—human resources (HR) records, legal workflows, personally identifiable information—could be collected by adversaries now and decrypted later.
- The General Data Protection Regulation's (GDPR) requirement for "appropriate technical measures" will mean quantum-resistant encryption by 2030.
- **This is not a future problem. The risk is present today.**

## Healthcare

Quantum computing offers immense potential in revolutionizing healthcare through accelerated drug discovery and personalized medicine. By simulating molecular structures and biological processes at unprecedented speeds, researchers can identify new drug candidates more rapidly and accurately, leading to faster development of treatments and cures for complex diseases. This capability extends to personalized medicine, where quantum computing can analyze genetic data to tailor treatments to individual patients' unique profiles, enhancing efficacy and reducing adverse effects.

## Supply chain

Quantum computing will dramatically enhance supply chain management and logistics optimization. With its ability to solve complex optimization problems and process vast amounts of data in real time, quantum computing can identify the most efficient routes, predict and mitigate potential disruptions, and optimize inventory levels. This leads to significant cost savings, improved delivery times, and increased operational efficiency, providing a competitive advantage to organizations in manufacturing, retail, and distribution.

## Finance

In finance, quantum computing will detect and prevent fraud with unprecedented accuracy by analyzing complex transaction patterns and identifying anomalies in real time. Quantum algorithms will optimize investment portfolios and manage financial risks more effectively, leading to better decision-making and enhanced profitability. In insurance, quantum computing will enhance risk assessment and underwriting processes by processing vast amounts of data, leading to more accurate predictions and personalized insurance products, thereby improving customer satisfaction and operational efficiency.

## Technology, media, and telecommunications

Quantum computing is poised to redefine capabilities within the technology, media, and telecommunications sector by enhancing data processing and analysis. In technology, quantum computing can accelerate advancements in artificial intelligence, enabling machines to learn and adapt more efficiently, which drives innovation in software development and cloud computing services. For media companies, quantum algorithms can analyze consumer data at scale, leading to highly personalized content delivery and more effective advertising strategies. Telecommunications will benefit from enhanced network optimization and more efficient data routing, improving connectivity and service delivery for consumers. The sector as a whole will see increased cybersecurity with quantum-resistant encryption methods to protect sensitive data and communications from evolving threats.

## Industrial manufacturing

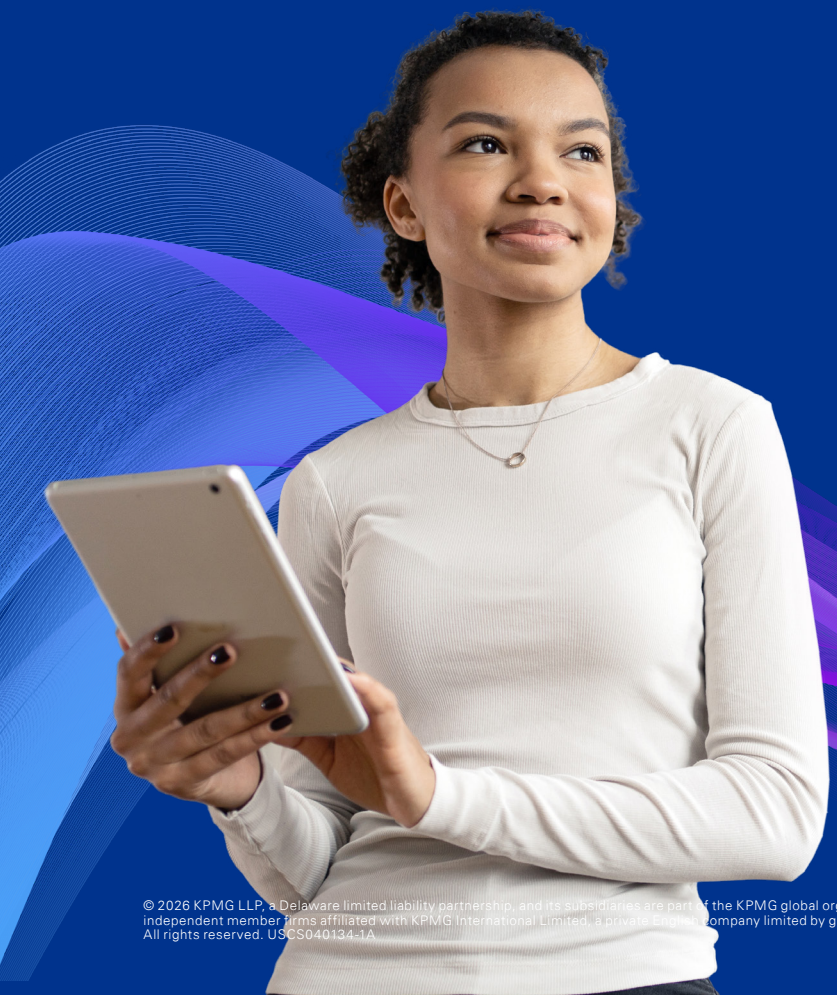
Quantum computing offers transformative potential in industrial manufacturing by optimizing complex supply chains and manufacturing processes. By solving intricate optimization problems rapidly, quantum computing can enhance production efficiency, reduce waste, and minimize costs, leading to higher-quality product development and faster time-to-market. The capability to model and simulate material behaviors at the atomic level can spur innovation in developing new materials with improved properties, enhancing the durability and functionality of manufactured goods. Manufacturers can further leverage quantum computing to predict maintenance needs and reduce downtime in production lines, improving operational efficiency.

## Energy, natural resources, and chemicals

The energy, natural resources, and chemicals sector stands to gain significantly from quantum computing in areas such as resource exploration, energy production, and materials discovery. Quantum computing can analyze vast datasets to identify new energy reserves, optimize extraction processes, and improve resource allocation, enhancing efficiency and sustainability. In chemical engineering, simulating molecular interactions at a quantum level can accelerate the development of novel compounds and catalysts, leading to breakthroughs in environmental conservation and energy storage. Energy providers can use quantum computing to forecast consumption patterns more accurately and optimize grid distribution, reducing waste and improving resilience in energy supplies. Additionally, advancements in quantum encryption will strengthen the security of critical infrastructure and protect against cyber threats.

# Postquantum cryptography: Managing risk

The migration to postquantum cryptography (PQC) is critically important for all organizations to maintain the security and integrity of their valuable data and personal information in the face of emerging quantum computing threats. Such threats could potentially break current cryptographic algorithms, exposing valuable data to unauthorized access. Starting the transition to PQC now is essential to safeguard against the "harvest now, decrypt later" threat model, where adversaries collect encrypted data with the intention to decrypt it once quantum capabilities become viable. Preparing proactively will not only protect your organization's information assets but also ensure compliance with upcoming regulatory requirements, fortify its defenses against future threats, and demonstrate a commitment to advanced security measures, thereby maintaining trust with their customers.



### The clock has a deadline—and it affects your data

Governments and standards bodies have already published hard deadlines for phasing out the encryption your vendors use today. This isn't theoretical—it's regulatory. What this means for privacy includes:

### Harvest now, decrypt later

Adversaries—mostly nation-states—have been collecting encrypted data since at least 2015. They store it and wait. When quantum computers become commercially available (projected 2028–2033), they will decrypt it. Any personal data, contract data, or confidential records transmitted through your enterprise today could be in someone's vault right now.

### GDPR Article 32 has a quantum dimension

The obligation to apply "appropriate technical measures" for data protection will require quantum-resistant encryption by 2030. Organizations that haven't transitioned may face regulatory exposure—not because of a breach that happened tomorrow, but because of data collected years ago.

### Data with long retention = highest risk

HR records, audit trails, legal documents, financial data—anything your organization needs to keep confidential for 10 or more years is the most vulnerable category. Prioritize these.

# Deprecation and end of life: The clock is ticking

| Algorithm type | Algorithm/Standard | Deprecated by | Disallowed by |
|---|---|---|---|
| Digital signature algorithms | ECDSA 112 bits security strength | 2030 | 2035 |
| | ECDSA ≥ 128 bits security strength | - | 2035 |
| | EdDSA ≥ 128 bits security strength | - | 2035 |
| | RSA 112 bits security strength | 2030 | 2035 |
| | RSA ≥ 128 bits security strength | - | 2035 |
| | ECDSA (all parameter sets) | - | 2035 |
| | EdDSA (all parameter sets) | - | 2035 |
| | RSA (all parameter sets) | - | 2035 |
| Key establishment schemes | Finite field DH 112 bits security strength | 2030 | 2035 |
| | Finite field MQV 112 bits security strength | 2030 | 2035 |
| | RSA 112 bits security strength | 2030 | 2035 |
| | Finite field DH ≥ 128 bits security strength | - | 2035 |
| | Finite field MQV ≥ 128 bits security strength | - | 2035 |
| | RSA ≥ 128 bits security strength | - | 2035 |
| Symmetric cryptography | Symmetric standards at 112 bits security level | n/a | 2030 |

# What should organizations do to prepare?

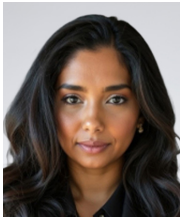
Three things privacy teams should do right now:

1. *Get a seat at the PQC table*—PQC migration is being led by security and information technology teams—but it has direct privacy consequences. Privacy leaders need to be part of the conversation, not briefed after decisions are made. This means working with your crypto officer and data governance teams to make sure long-lived sensitive data is prioritized in the transition plan.
2. *Extend your data classification to include "quantum risk"*—Review your data retention and classification policies with a quantum lens. Any data that must remain confidential beyond 2030 should be flagged for priority re-encryption with quantum-resistant algorithms.
3. *Update your privacy impact assessments and vendor reviews*—GDPR data protection impact assessments (DPIAs) and records of processing activities should now include a quantum risk question: "Is this data encrypted in a way that will remain secure beyond 2030?" Third-party data-sharing agreements—including with your major Software-as-a-Service vendors and their subprocessors—should be reviewed to ensure quantum-resistant encryption is part of the roadmap.

The KPMG Q-PREP program gives organizations a structured, seven-step path to quantum readiness—starting with a cryptographic asset inventory and risk assessment, through to full PQC migration and continuous monitoring. We can also provide plain-language privacy briefings, DPIA templates with quantum considerations, and vendor assessment frameworks. Quantum-resistant encryption is part of the roadmap.

# Contact us

**Dr. Aaron Kemp**
**US Quantum Lead,**
**KPMG LLP**
**T:** 404-358-3138
**E:** aaronkemp@kpmg.com



**Dr. Lekshmy Sankar**
**US Quantum Security Lead,**
**KPMG LLP**
**T:** 303-495-8125
**E:** lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**Learn about us:** **kpmg.com**