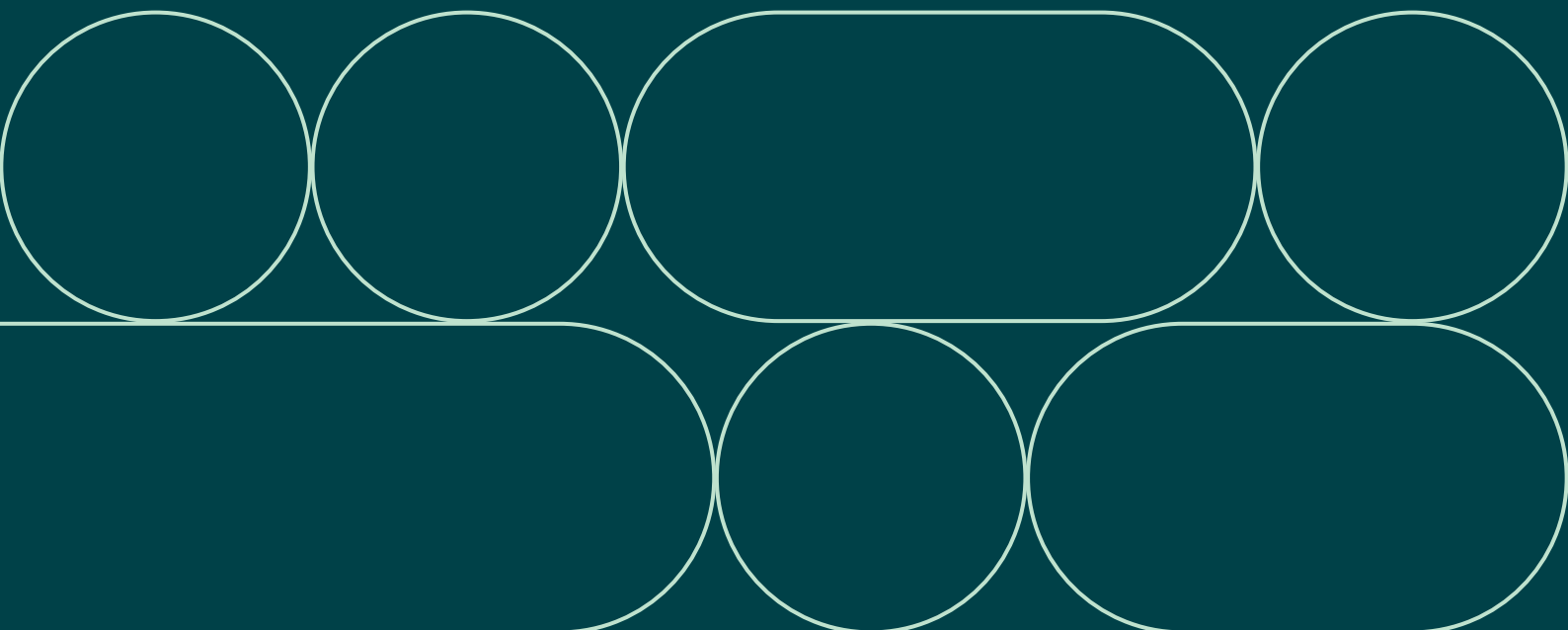
CROWN INFORMATION MANAGEMENT

Addressing the Privacy Operations Solutions Gap

A Guide for DPO Teams

Work uncomplicated

crownrms.com ↘



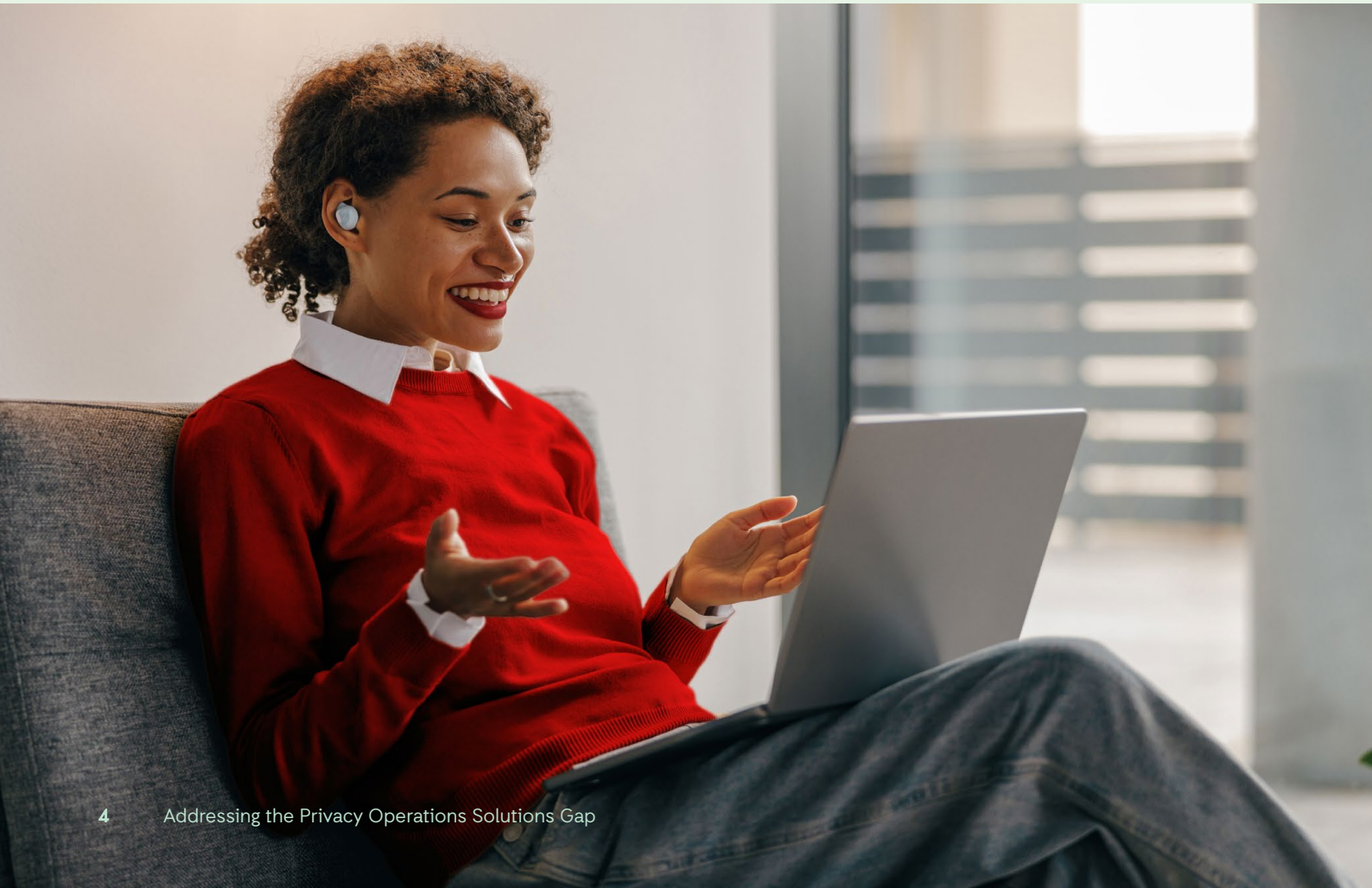
Contents

Executive Summary

Organisations across the UK and European Union face increasing regulatory pressure to demonstrate control over personal data throughout its lifecycle. The EU General Data Protection Regulation (GDPR) and UK GDPR impose strict obligations on organisations to ensure personal data is processed lawfully, securely, and transparently.

Key regulatory principles including Accountability (Article 5(2)), Data Protection by Design and Default (Article 25), Security of Processing (Article 32), and Records of Processing Activities (Article 30) require organisations not only to establish governance frameworks but also to demonstrate operational capability across complex information ecosystems.

Modern organisations operate across fragmented environments including legacy enterprise systems, cloud platforms, collaboration tools, analytics environments, and physical archives. As a result, Data Protection Officers (DPOs) are accountable for compliance but often lack direct operational visibility across the systems that store and process personal data.



Market Reality and Regulatory Pressure

Regulators increasingly focus on operational evidence of compliance rather than policy statements alone. The GDPR accountability principle (Article 5(2)) requires organisations to demonstrate compliance with core principles such as lawfulness, transparency, data minimisation and storage limitation.

Article 30 requires organisations to maintain Records of Processing Activities (RoPA), including categories of personal data processed, processing purposes, recipients, retention periods and security measures. Maintaining accurate RoPA documentation requires organisations to understand where personal data resides across systems.

Article 15 establishes the right of access (DSAR), giving individuals the right to obtain confirmation whether their personal data is processed and to receive copies of that data. Organisations must respond within one month under both EU and UK GDPR.

Market evidence highlights the scale of the challenge:

IDC estimates global data volumes will exceed 175 zettabytes by 2025.

Gartner reports that more than 80% of organisations lack a complete view of enterprise data assets

Since 2018 regulators have issued more than €4 billion in GDPR fines.

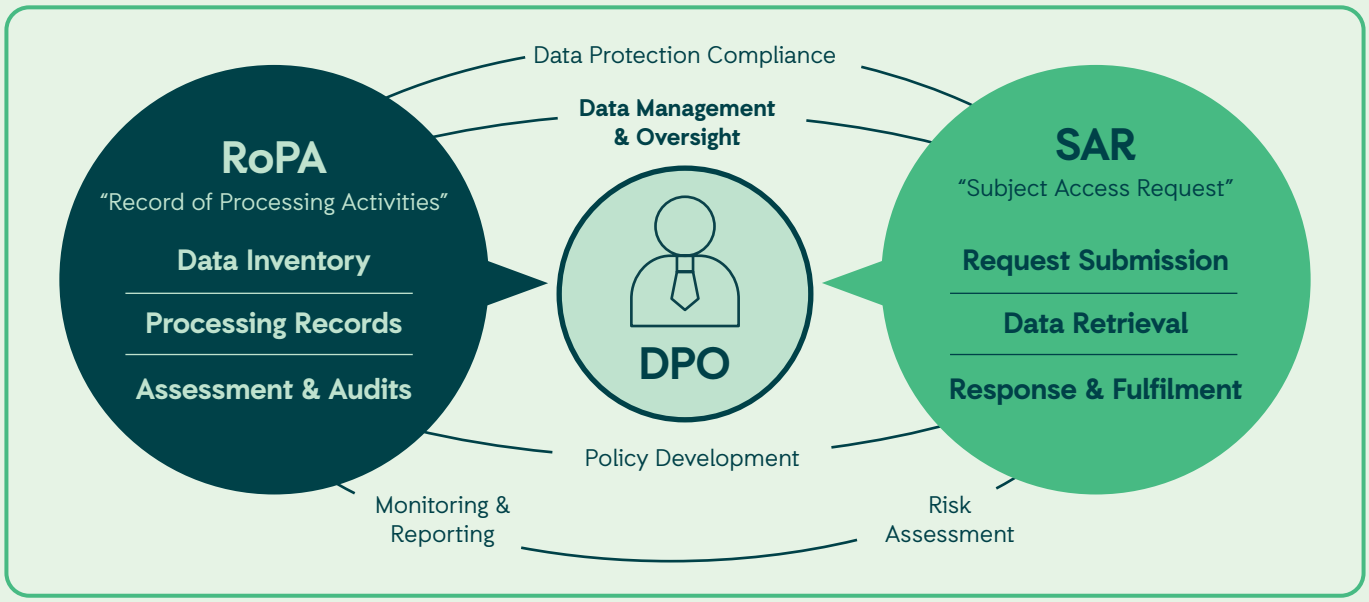
The European Data Protection Board reports that DSAR complaints are among the most common privacy complaints.

The Privacy Operations Gap

In many organisations privacy governance has evolved faster than operational capability. While DPOs are responsible for monitoring compliance and advising on data protection obligations under Article 39 GDPR, the underlying data infrastructure is typically managed by IT teams, product development groups, analytics teams and information governance departments.

DPO Teams often lack direct or even indirect control over the very sources of data for which they are required to exercise regulatory oversight.

- IT architecture
- Data storage environments
- Digital product design
- Information lifecycle governance



This structural disconnect creates what we define as the **Privacy Operations Solutions Gap**.

DPO Accountability

Operational Gap

Digital Systems & Data Infrastructure

This fragmentation creates a structural governance challenge. Privacy teams often rely on manual searches, incomplete data inventories and departmental knowledge to respond to regulatory requests. Technology solutions in this space are often repurposed from legacy document processing. They can depend heavily on manual processes, lack integration with the wider data landscape, and overlook archived data that exists across almost every organisation. The result is a gap between regulatory accountability and operational visibility — the Privacy Operations Solutions Gap.

The Hidden Complexity of the Data Supply Chain

Personal data moves across multiple stages during its lifecycle including creation, operational processing, analytics use, archiving and disposal. These stages span both digital systems and physical records environments.

01

Data Minimisation (Article 5(1)(c)) requires that personal data must be limited to what is necessary for the purposes for which it is processed.

In practice, organisations often maintain decades of accumulated data across legacy systems, archives and duplicated digital environments. Without unified visibility across this supply chain it becomes extremely difficult to apply consistent retention policies or implement Privacy by Design.

Industry Case Studies

Financial Services

A multinational financial services organisation experienced a 300% increase in Data Subject Access Requests following regulatory scrutiny. Manual searches across more than 40 systems resulted in response times exceeding 35 days. Implementing integrated discovery and archive visibility reduced response times by more than 60% and improved auditability.

Healthcare

A healthcare provider managing millions of patient records struggled to locate historical medical documentation across legacy databases and physical archives. Improved lifecycle governance and system discovery strengthened regulatory response capabilities.

Public Sector

A government agency responding to FOI and subject access requests required visibility across decades of paper archives and digital systems. Structured archive management and discovery processes significantly improved response timelines.

Retail

A multinational retailer struggled to map customer data across e-commerce platforms, CRM systems and marketing technologies. Improved data discovery allowed the organisation to create a unified inventory of personal data sources and better manage consent and DSAR responses.

The Quantra–Crown Privacy Operations Framework

The Quantra–Crown Privacy Operations Framework integrates privacy governance, operational technology and information lifecycle management.

Privacy Governance Layer

DPO oversight, regulatory policy and compliance monitoring aligned with Articles 24 and 39 GDPR.

Privacy Operations Layer

Quantra platform supporting DSAR workflows, RoPA management and DPIA orchestration.

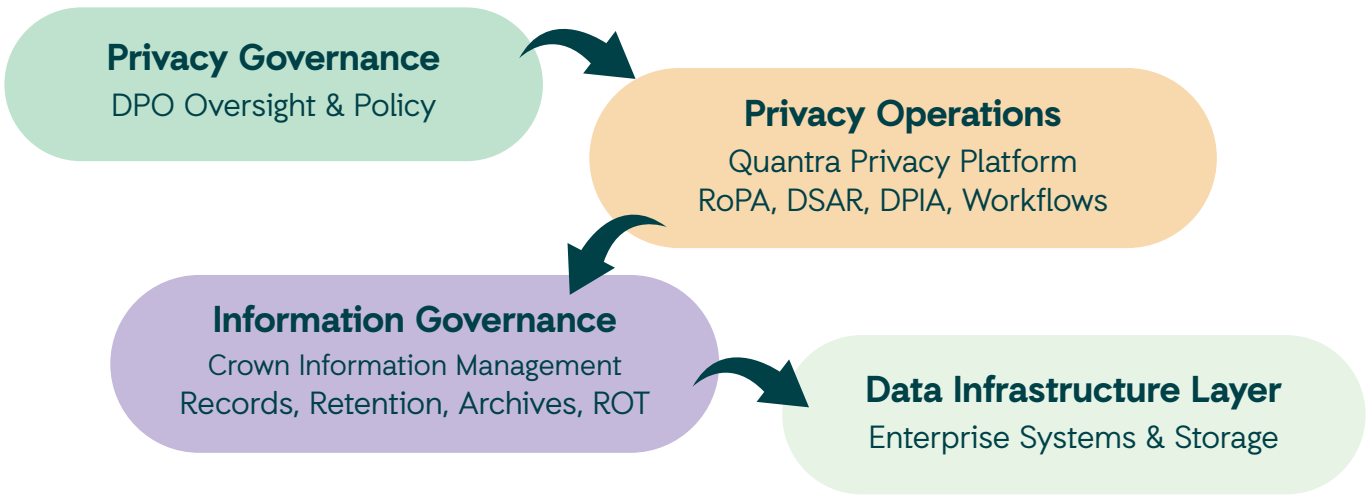
Information Governance Layer

Crown Information Management providing records management, retention governance and secure archive services.

Data Infrastructure Layer

Enterprise systems, cloud platforms and analytics environments where personal data resides.

The Quantra–Crown Privacy Operations Framework



Operational Benefits of Integrated Privacy Operations

Integrated privacy operations provide measurable operational benefits and support progression towards greater privacy operations maturity (levels 4 & 5):

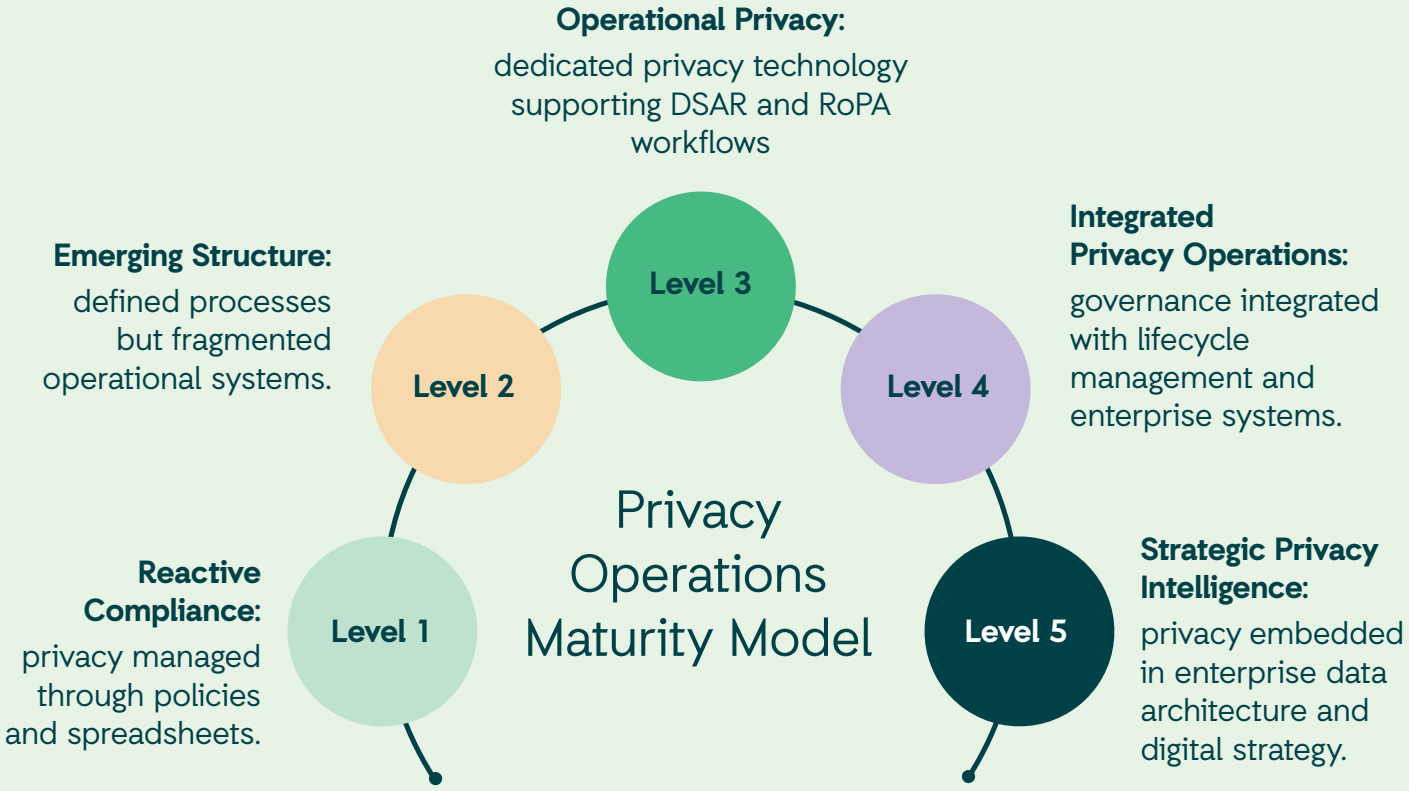
01
Faster DSAR responses through automated system discovery

02
Reduced regulatory risk through improved visibility across data environments

03
Stronger lifecycle governance and retention management

04
Lower operational burden on IT, legal and compliance teams

05
Improved auditability and evidence of GDPR accountability



The Way Forward

Assess the maturity of current privacy operations capabilities.

Map the full information supply chain including legacy systems and archived records.

Implement integrated discovery, governance and lifecycle management solutions to operationalise GDPR compliance.

Strategic Benefits of the Quantra–Crown Partnership

End-to-end visibility across the information estate

Quantra provides intelligent discovery and orchestration capabilities that identify where personal data is likely to exist across enterprise systems. It can then be extracted for DPO Team action, while Crown Information Management provides visibility and governance over archived and physical records environments.

This combined capability enables organisations to develop a complete operational view of their information estate, including legacy systems and historical archives that are frequently overlooked in privacy programmes.

Benefit:

Organisations gain the ability to locate, retrieve and govern personal data across both digital and physical environments — significantly reducing blind spots in regulatory searches.

Operationalising GDPR Accountability

GDPR requires organisations to demonstrate accountability for how personal data is processed. In practice, this means being able to provide evidence of how data is discovered, managed, retained and ultimately disposed of.

The Quantra–Crown framework enables organisations to operationalise this requirement by combining automated data discovery, structured privacy workflows, lifecycle governance and retention management.

Benefit:

Organisations move beyond policy-based compliance and establish repeatable operational processes that demonstrate GDPR accountability in practice.

Faster and more reliable DSAR response

Data Subject Access Requests remain one of the most operationally demanding obligations under GDPR.

By integrating discovery across enterprise systems with structured archive management, the Quantra–Crown approach enables privacy teams to quickly identify where relevant data, including handwritten data elements, is likely to reside. This data can then be extracted and provided to DPO teams via the Quantra inventory and workbench for onward processing in line with privacy obligations.

Benefit:

DSAR response processes become significantly faster, more consistent and more defensible during regulatory scrutiny.

Reducing data risk through lifecycle governance

A major source of privacy risk arises from excessive data retention and uncontrolled data duplication across systems.

Crown's information lifecycle governance capabilities ensure that records are managed according to structured retention schedules and regulatory requirements, while Quantra provides visibility across the environments where personal data exists.

Benefit:

Organisations reduce regulatory exposure by ensuring that personal data is retained only where necessary and disposed of appropriately.

Enabling privacy at enterprise scale

Modern organisations operate across increasingly complex digital ecosystems that include cloud services, SaaS platforms, legacy applications and data analytics environments.

Quantra's metadata-driven architecture enables discovery across distributed environments without centralising sensitive datasets. Combined with Crown's information governance capabilities, organisations gain scalable privacy operations infrastructure across modern digital environments and historical archives.

Benefit:

Privacy governance becomes scalable across the entire enterprise — supporting digital transformation while maintaining regulatory compliance.

From Privacy Governance to Privacy Operations

For most organisations, privacy governance is already well established. Policies exist, compliance frameworks are in place, and Data Protection Officers actively monitor regulatory obligations. The challenge now is operational.

Organisations must ensure that privacy governance is supported by the infrastructure, processes and visibility required to manage personal data at enterprise scale.

This requires moving beyond fragmented approaches to data discovery and information management and adopting a more integrated model of privacy operations.

Building confidence in the information supply chain

At its core, privacy governance depends on one fundamental capability: confidence in the organisation's ability to understand and control its information supply chain.

Organisations must be able to answer critical questions with confidence:

The Quantra–Crown partnership enables organisations to answer these questions by bringing together intelligent data discovery, operational privacy workflows, enterprise information governance, and lifecycle management across digital and physical records.

Turning privacy into a strategic capability

Rather than viewing privacy solely as a regulatory obligation, forward-looking organisations are beginning to treat it as a strategic capability that strengthens trust, improves governance and supports responsible data innovation.

By implementing integrated privacy operations infrastructure, organisations can:

Strengthen regulatory confidence

Reduce operational risk

Improve data governance

Enable responsible use of data across the enterprise

The opportunity ahead

Privacy regulation will continue to evolve, data volumes will continue to grow, and enterprise data environments will only become more complex.

Organisations that invest in operational privacy capabilities today will be far better positioned to navigate this future with confidence.

The Quantra–Crown partnership provides the foundation for this transformation — enabling organisations to move from fragmented privacy processes to a unified operational model of privacy governance across the entire information lifecycle.

Crown Information Management help clients to maximise the value of their "corporate memory" through the storage, active management and timely distribution of information assets.

In 40 countries, Crown provides secure archiving and retrieval of information in physical and electronic format, as well as digital imaging, media management and data destruction.

Work uncomplicated
crownrms.com ↘

Discover Crown

A complete range of services to support you and your business

crownworldwide.com

- World Mobility
- Relocations
- Information Management
- Fine Art
- Logistics
- Workspace