Privacy and Security

How can we balance conflicting regulatory obligations around data, privacy and security?

Over the past decade financial services firms have faced an onslaught of privacy and security regulations. Data protection has rapidly shifted from a niche topic of conversation to a board meeting agenda item in all financial institutions. While increased consumer safeguards are welcomed, heightened focus on data protection has created a new set of challenges for information governance.

For Records Managers, who previously had little involvement in the governance of data contained within records, conflicting data privacy and security obligations have resulted in a risky balancing act that decades-old systems and process are ill-equipped to handle.

For Data Officers on a mission to enhance data-driven business growth, and for Security Officers trying to forge strong and secure connections between departments and jurisdictions, new governance mandates around privacy and data protection have been a major distraction.

Today, all internal stakeholders are concerned with

- understanding which information assets are held by your organization, and where
- verifying which regulations apply to these information assets, and identifying the records and data governance obligations associated with them, whichever jurisdiction they reside in
- monitoring rules and regulations across all jurisdictions, understanding the impact of regulatory change on your records and data, and taking remedial action in a timely manner
- knowing which records contain personal data, and how that data must be managed, either within or separate from the record itself

- putting procedures and controls in place to safeguard personal data and monitor compliance
- storing data within records in the right location, subject to the procedures and controls required for effective governance
- protecting these records securely and compliantly in transit, as they cross borders, from one jurisdiction to another
- interpreting rules and regulations, and recognizing when data protection obligations conflict with security and recordkeeping requirements
- making risk-based assessments to determine the most compliant course of action to take when conflicts arise
- accelerating e-discovery, enabling records containing personal data to be located quickly, when required for a litigation or compliance investigation, or when a former customer invokes their right to be forgotten
- creating a defensible audit trail to track and manage data within records, and other information assets

Two million customer staff consume regulatory intelligence, in 180 countries and 60 languages, powered by CUBE

Use case: The CUBE approach to GDPR

The General Data Protection Regulation (GDPR), operating alongside other new data privacy regulation such as the California Consumer Privacy Act (CCPA), has disrupted life for information governance practitioners.

CUBE is working with financial services firms to

- **Establish, distribute and execute policy, consistently across the enterprise**

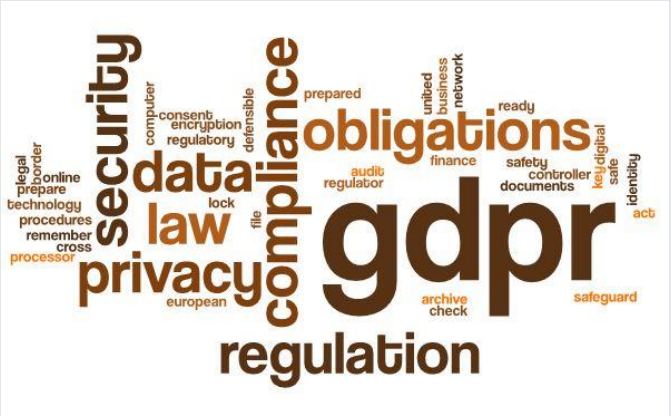
  CUBE provides a single view of regulatory obligations across all record types and jurisdictions. Records are tagged with all relevant regulations, across all regions, ensuring that when policy is set or reviewed (for retention, for example), all applicable obligations are fully understood.

  Globally and regionally, CUBE manages policy distribution across the business and monitors for consistent execution across the enterprise. CUBE knows when GDPR is superseded by, or conflicts with other regulations (MIFID II or FINRA, for example), enabling risk-based assessments to help you determine the most compliant course of action. Scenarios like this can be managed automatically in accordance with policy, by rules-based workflows, to ensure regulatory compliance.

- **Determine the right time to destroy records containing personal data**

  GDPR stipulates that personal data must be destroyed as soon as the regulatory retention obligation has been met, unless there is a strong and valid justification for keeping it. This is in stark contrast to the historical tendency to keep the majority of records, forever.

  CUBE inventory maps metadata within your records and tags them with identifiers (personal data, for example). With CUBE, you know where all of the personal data within your organization lies, and you know your retention obligations in relation to each record type, enabling informed and compliant decisions when determining the right time for disposition.



- **Enable cross-border personal data transfer without compromising privacy or security**

  GDPR concerns data protection and privacy for all individuals with the European Union (EU) and European Economic Area (EEA), as well as the export of data outside of these regions. Cross-border data transfer is a major compliance risk for firms with multi-jurisdictional operations.

  By classifying all records to identify those that contain personal data, and by mapping all global regulations onto all policy, procedures, controls and records, CUBE automatically knows exactly which records are a GDPR compliance risk as they pass from one jurisdiction to another. Alerts are issued in real time, when compliance breaches are detected, enabling timely remediation and avoidance of enforcement fines.

- **Create a defensible audit trail**

  GDPR and other privacy regulations are relatively new. Global regulators appreciate the extent of change involved and are eager to work with financial institutions to ensure compliance.

  CUBE automatically records a thorough and easy to access audit trail that details how privacy-related policy has been set and executed, how records containing personal data have been managed and what decision rationale has been applied throughout your journey towards compliance.

Book your 10-minute discovery call to find out how CUBE will work for you
contact@cube.global
www.cube.global