WHITE PAPER

MACRO|4
A Division of UNICOM® Global

COLUMBUS FOR INFORMATION GOVERNANCE

Turning compliance into competitive advantage

www.macro4.com

Contents

Information governance challenges through 2023 and beyond

Sound information governance is the mark of a well-run organization. But it is a greater challenge than ever before – and the stakes are high.

The huge GDPR fines and adverse publicity for Meta, Amazon and others found breaking data protection rules demonstrate just how important it is for business executives to take information governance seriously.

Information governance is about much more than simply managing information, or handling regulatory compliance. Crucially, it requires organizations to develop a strategy to protect information, leverage it responsibly and build customer trust. Information governance is a discipline which involves employees at all levels following consistent policies and processes to maintain best practice in the face of different – sometimes conflicting – demands from customers, regulators, legislators and internal stakeholders.

Cyber security is the foundation on which all other information governance measures are built and it remains a top challenge for 2023. Enterprises around the globe must respond to unprecedented threats from criminals intent on infiltrating IT systems and stealing or tampering with enterprise information.

New data protection laws are also continuing to bite. The EU's General Data Protection Regulation (GDPR) has caused a seismic change in data privacy practices since its introduction in May 2018. The US has strengthened data protection with a slew of new laws at state level, most notably the California Consumer Privacy Act (CCPA), and most recently the UK government set out its own proposed regulations in the Data Protection and Digital Information Bill (DPDIB). Across the world, governments of all political persuasions are introducing tougher data privacy legislation, with better enforcement and stiff fines for violations. Sector-specific regulation also continues to expand, creating more complexity and uncertainty. Faced with compliance challenges on multiple fronts, organizations must continue to improve their processes and systems for compliance management, monitoring and reporting.

The role of EIM in information governance

Enterprise information management (EIM) systems have a vital role to play in controlling and organizing the huge variety and volume of data flowing through the enterprise, as part of a company's overall information governance strategy.

EIM systems are designed to manage information at scale: an essential requirement as data growth continues to explode. According to market intelligence provider IDC[1], worldwide data will grow by 61 per cent annually to reach a total of 175 zettabytes by 2025 – the equivalent of 12.5 billion of today's largest hard drives. Additionally, IDC[2] estimates that 80 per cent of this information will be unstructured. This is where an EIM system comes into its own.

Bringing order to 'disorderly' data

Unstructured data poses a particular challenge because it is 'disorderly'. Unlike the data found in traditional databases it is not logically structured, exactly as the name implies. Unstructured data exists in multiple formats, layouts and locations, making it much harder to control.

EIM brings order to the chaos caused by this disorderly, unstructured data. Information can be automatically captured, classified and processed regardless of its format or origin – from documents, images and video to voice recordings, chat logs and SMS messages, as well as data records from business applications. Business rules-based automation minimizes costs and manual effort and reduces the incidence of human errors that can lead to compliance violations.

Information governance solutions

Columbus from Macro 4 is a highly scalable enterprise information management suite comprising content services, workflow, compliant data storage and multi-channel delivery.

Businesses across the globe use Columbus to organize their unstructured data, automate information management tasks and reduce the costs, risks and effort involved in information governance. Workflow ensures that the right information is available to the right person, in the right place, at the right time. Encryption, tamper proofing, identity management and data segregation keep information secure at every stage.

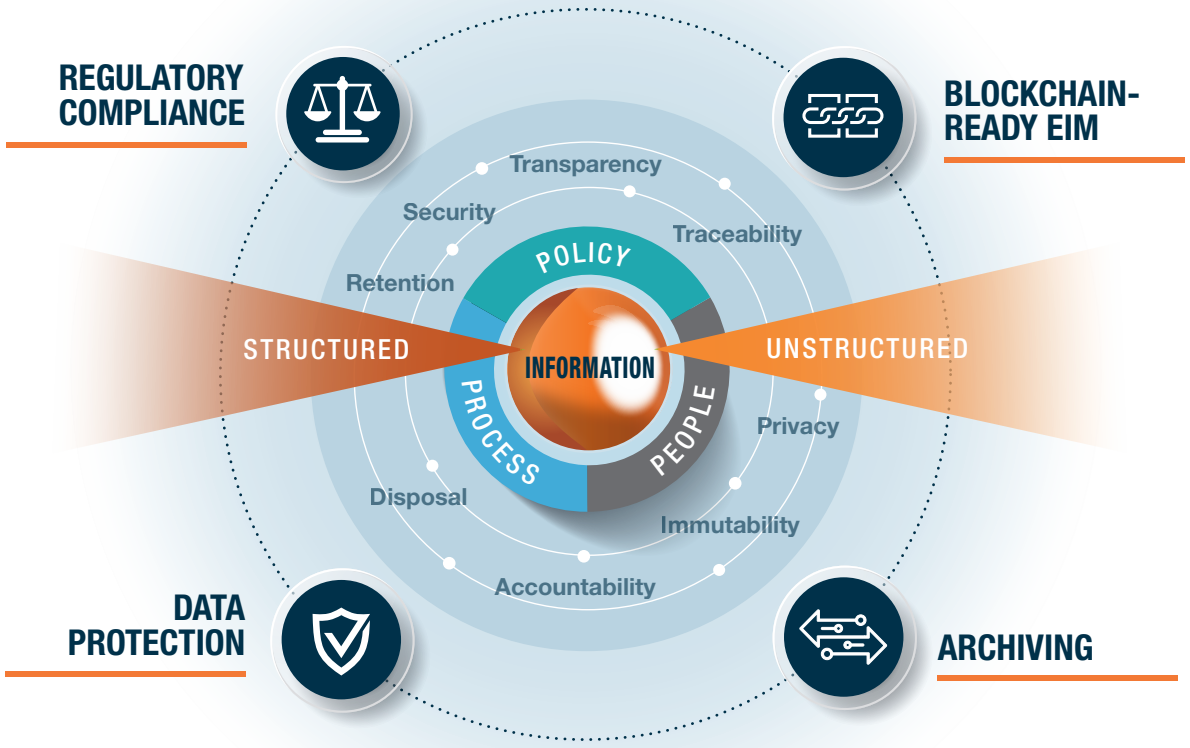
[1] IDC: Data Age 2025, The Digitization of the World from Edge to Core, 2018

[2] IDC/Solutions Review: 80 Percent of Your Data Will Be Unstructured in Five Years, 2019

Supported by Columbus, organizations can maintain highly effective and robust information management practices which build trust and customer loyalty. Today's consumers are increasingly savvy when it comes to data protection, so the ability to demonstrate that their personal information is handled responsibly is an important competitive differentiator.

Macro 4 has a twenty year track record in delivering information management solutions to organizations operating in all major compliance regimes and industry sectors. Macro 4 offers tailored solutions, implemented by professional services specialists, to address its customers' unique governance challenges. Additionally, focused solutions are available for regulatory compliance, blockchain-ready EIM, data protection and archiving.

INFORMATION GOVERNANCE IN ACTION



A CHANGING REGULATORY LANDSCAPE

Regulatory change is now the norm, with no sector spared from growing demands for organizational accountability, transparency and oversight.

To keep in line with data protection regulations, enterprises must follow strict rules governing the use of customer and employee information. These rules include maintaining high security levels, minimizing exposure of sensitive content, and fulfilling individuals' requests for accessing or deleting their personal data. Looking beyond personal data there are hundreds of industry-focused and region-specific regulatory regimes focused on accountability, fairness and transparency in business transactions and practices.

Common to most regulatory systems are requirements for:

- Compliance monitoring and breach detection
- Auditing of compliance processes and regulatory reporting
- Preservation of evidence through records management, non-repudiation measures and legal hold

Solutions for regulatory compliance

The Columbus suite provides information lifecycle management and records management capabilities to handle the creation, classification, use, retention and disposal of information in line with an organization's compliance obligations.

Documents and other relevant information are secured to provide tamper-evident proof of business activities and transactions. Content can be generated in a wide range of formats for compliance purposes. For example, EU-compliant PDF and/or XML invoices can be created which meet ZUGFeRD, XRechnung and Factur-X standards. Items can also be placed under legal hold to prevent further processing in the event of litigation.

Columbus is well suited for use in high security settings such as law enforcement, where it can maintain the chain of custody for digital evidence such as police bodycam footage in criminal cases. All activity relating to an item of information – such as how it has been processed, accessed or distributed – is recorded in a secure audit trail, using blockchain-ready cryptography to prevent tampering (see also 'Blockchain-ready EIM', below).

Document workflows are managed and monitored centrally, with automated alerts to prompt investigation of non-compliant or suspicious system activity, and comprehensive reporting to meet the needs of regulators and business stakeholders. Business processes can be mapped using workflow and updated quickly in response to changes in government legislation and industry regulations.

Columbus data security and privacy features

Granular security and access controls provide the highest levels of protection for business information, and data privacy features can be used to limit the exposure of sensitive or personal data.

- **Identity and access management (IAM)**
  Columbus supports strong user authentication, and integrates with third party IAM systems to enable multi-factor authentication (MFA), biometrics, digital signatures and location awareness; access rights can be controlled down to individual field level, based on a range of user characteristics

- **Data segregation**
  For physical security or compliance, data may be stored in multiple physical locations and on a variety of storage media, with access controlled centrally

- **Secure storage**
  Columbus provides secure, tamper-evident and encrypted data storage and supports storage on tamper-evident hardware; blockchain-ready cryptography and auditing mechanisms ensure data immutability

- **Data redaction**
  Data can be selectively redacted at viewing time to prevent exposure of personal information except where essential, for example in customer service

- **Data disguising**
  To protect individual confidentiality, for example when using personal information for statistical purposes, data can either be completely anonymized or, alternatively, pseudonymized; pseudonymization allows organizations to replace names and other personal identifiers with a non-identifying equivalent, such as a code, which can be linked back to the individual later if required

Decommissioning legacy content repositories

Legacy content repositories often lack the necessary security and privacy features to adequately protect business data and meet today's information governance standards. Data from these repositories can be quickly migrated to Columbus, and the original system retired. This ensures a compliant approach to data protection, with the flexibility to adapt to future compliance requirements, and also eliminates the costs of supporting multiple content management systems.

CASE STUDY

Redacting sensitive customer data for Open Banking

As part of the Open Banking initiative, a large, UK-based provider of retail financial services needed to find a way to exchange customer data with other regulated providers while maintaining compliance with all regulatory standards.

In order to comply with the Payment Card Industry Data Security Standard (PCI DSS) when sharing information on behalf of its customers, the bank needed to remove sensitive credit and debit card data, such as the primary account number (PAN), from its files.

The bank used the redaction capability in Columbus to replace the sensitive data with black boxes. This was a very simple solution which could be applied selectively and automatically, based on business rules. It avoided the need for the bank to make any changes to its core banking systems or pay a third-party supplier to change the layout of its electronic documents.

BLOCKCHAIN: A TOOL FOR COMPLIANCE

Blockchain technology has huge potential for managing compliance due to its immutability; once data has been saved onto the chain it is practically impossible to change or delete. Significant transactions, documents and actions can all be written to the chain to provide a trusted record of events.

Blockchain networks are also useful for reporting on compliance activities in real time. This reduces the need for manual data collection and eases the burden of regulatory reporting for enterprises and regulators alike.

In addition, blockchain networks support faster identity checks and reduce the wait for customers in 'know your customer' (KYC) and anti-money laundering (AML) processes by allowing multiple participants – such as banks and their customers – to share and validate data.

Despite the growing interest in blockchain for compliance, many business leaders remain cautious about making major investments in the technology. Organizations operating in regulated industries are seeking ways to make use of blockchain networks without making significant changes to their existing IT infrastructure.

Columbus provides that capability.

Blockchain-ready EIM

Columbus is the first 'blockchain ready' enterprise information management system.

The Columbus software uses the same cryptographic mechanisms as the blockchain to capture and record its internal system events in a tamper-evident audit trail. This approach ensures immutability for information stored in the Columbus repository. It also proves exactly how that information has been used, by whom and when.

Additionally, the Columbus suite integrates with the Hyperledger blockchain framework to provide a second immutable record – with all the non-repudiation features of distributed ledger technology applied. This approach allows a practically limitless range of data to be exchanged seamlessly with blockchain networks and shared with regulators, auditors, customers and other participants in regulatory processes. Organizations can deliver absolute proof that compliance processes have been followed correctly – such as preventing unauthorized access, or deleting a customer's personal data in response to a request for erasure.

USE CASE

A blockchain solution for the 'right to be forgotten'

When it comes to customers exercising their right to erasure – known as the 'right to be forgotten' (RTBF) under the GDPR and the 'right to deletion' under the CCPA – compliance specialists are facing a conundrum. How do you provide conclusive documentary proof that a customer's data has been deleted without leaving a record that can be tied back to the customer in some way?

The following example from the banking sector illustrates how blockchain technology can provide evidence of compliance with a request for erasure without leaving behind any traces of the customer's personal data.

First, the bank creates a case ID for the request on its case management system and shares this with the customer. The customer's data is then deleted and an audit trail is written to the blockchain network, recording all of the steps the bank has taken to purge the data from its systems. This record is associated with the same case ID. The bank then notifies the customer that the case is closed and all remaining records of the case (including the case ID) are destroyed.

By this point only the customer knows the case ID. At a future date the customer could query the blockchain system using the case ID and view an audit trail of the erasure process, or ask a regulator to do so on their behalf. In this way, the integrity of the deletion process is maintained, while allowing checks to confirm that the request for erasure has been successfully completed.

THE GDPR AND CCPA: RAISING THE BAR FOR DATA PROTECTION

The GDPR governs how organizations around the world are permitted to collect, store and use the personal data of EU residents. Introduced by the European Union in 2018, the GDPR replaced the 1995 Data Protection Directive and brought in strict new data protection rules and greater financial penalties for violations. Companies who fail to comply face fines of up to 20 million or four per cent of global annual turnover for the previous financial year, whichever is higher.

While the CCPA 'only' applies to companies operating in California and handling the data of Californian residents, impact will be felt globally due to California's status as the world's fifth largest economy. Although similar to the GDPR in many respects, the CCPA has a strong focus on limiting the selling of personal data. Fines are low in comparison with the GDPR (up to $7,500 for an intentional violation), but individual consumers could claim up to $750 per incident through a lawsuit. In the event of a large-scale privacy breach that could amount to millions of dollars.

The GDPR and CCPA strengthen the rights of the individual and set out key data protection obligations for organizations that process personal data. These include greater transparency about how personal information is being used; responding quickly to customer requests to access, move or delete their personal data (within one month for the GDPR and 45 days for the CCPA); and preventing personal information from being used in ways the customer has objected to, or that breach individual privacy. Other new global data protection regulations are, in the main, adopting a similarly stringent approach. While the UK DPDIB deviates from the GDPR in some respects, it seeks to ensure data adequacy with the EU, and retains similar maximum penalties.

EU data protection penalties: the impact

The total fines issued under the GDPR to date total almost €2.8bn, with damage to public trust also having a severe financial impact.

GDPR infringements vary widely and include failing to comply with the rights of data subjects; losing computers containing personal information; and using ineffective physical storage for documents containing sensitive personal data. Article 32 of the GDPR specifically covers 'insufficient technical and organizational measures to ensure information security'; article 32 violations are one of the most frequent cause of fines.

Columbus EIM solutions assist organizations in complying with data protection requirements such as these by managing information centrally and applying advanced privacy and security measures, including strong authentication, tamper-evident storage and data redaction.

Solutions for data protection

Managing vast quantities of diverse customer information in line with tougher data protection obligations is an ongoing challenge. A Columbus solution gives organizations granular control of all forms of enterprise content and allows it to be managed, processed and stored in compliance with regulations such as the GDPR and CCPA, and to adapt as the global data protection landscape evolves.

Managing data access, portability and erasure

Research conducted by Macro 4 in 2023 revealed that IT leaders find processing GDPR queries takes up significant time and resources.

While most businesses have processes in place to manage GDPR requests, responding to them can be time consuming to due to difficulties pinpointing and collating personal information from a huge range of content stores, systems and data types around the business.

The Columbus suite helps organizations to improve the way they classify, collate and format information so that they can operate more efficiently and deliver a faster response to customers who wish to view their data, move it to another provider or have it deleted. Columbus enables data to be classified automatically so that it is more searchable. A multitude of classification criteria can be applied alongside basic categories such as data owner, content type, sensitivity level and required retention period. In addition, integration with analytics engines allows personal information to be identified from unstructured data that has not yet been classified.

Both the GDPR and the CCPA require businesses to supply data in portable formats that can be transferred easily to third-party suppliers. Columbus facilitates this process by transforming data from diverse sources into common formats such as PDF, CSV and XML.

Information lifecycle rules ensure that customer requests for access, erasure or transfer can be carried out automatically as long as they are not in breach of other, conflicting regulatory obligations.

Compliance monitoring, auditing and reporting

Columbus provides proactive, real-time monitoring of all activities related to personal data, such as access, processing and erasure and can pass evidence of potential compliance issues or suspicious activities, such as unusual access attempts, to security information and event management (SIEM) systems to prompt further investigation. Information can be shared with regulators and auditors on blockchain platforms to provide proof of compliance.

Data protection by design and by default: a GDPR imperative

Organizations are required to put in place technology and processes to follow GDPR data protection principles and safeguard individual rights. This requirement, known as 'data protection by design and by default', is met through data security and privacy measures built into the Columbus suite (see 'Solutions for regulatory compliance', above), which safeguard personal data over the long term.

Data minimization and retention management

Under GDPR rules, organizations may only retain the minimum amount of personal data necessary for processing, and for the shortest possible time. Columbus allows organizations to set data retention policies to manage data from cradle to grave and ensure that it is erased, both automatically and on request, when there is no longer a legitimate purpose for keeping it.

Key findings from a May 2023 survey of 100 IT decision makers in UK enterprises:

62%
Find processing GDPR queries takes up significant time and resources

72%
Forced to invest more resources in GDPR compliance due to hybrid working

44%
Feel that red tape created by the GDPR has hampered digital transformation

86%
Believe the GDPR must keep pace with AI, or risk becoming irrelevant

THE ROLE OF ARCHIVING IN INFORMATION GOVERNANCE

Long-term retention of structured and unstructured data is a critical component of governance and compliance

To meet legal and regulatory requirements, information such as historical financial records, contracts and other legal documents may need to be retained for several years; certain categories of data must be held throughout the lifetime of the customer or even in perpetuity.

Historical records may be required for servicing customer requests or for operational activities and, in this scenario, integrating archives with line of business applications is recommended to provide fast access for business users.

Archiving also has a technical performance dimension. A build-up of historical data in heavily used business applications may cause performance problems which are best addressed by archiving older or redundant data.

Next-generation archiving solutions

Macro 4's approach is to create a 'living' archive that is easy for business and IT teams to access and use as part of their day-to-day business operations.

The full range of enterprise content can be archived in the Columbus repository, including database records in addition to documents and other unstructured data. All archived information is held in a secure, unalterable format and managed in line with corporate retention and compliance policies through to disposal at end of life. Data is compressed, enabling billions of items to be secured and accessed from a single server.

Columbus integrates with line of business applications to deliver seamless user access to archived data. The archives provide a rich source of business data which can be analyzed using business intelligence platforms to deliver actionable insights.

Archiving data from in-house systems or third-party applications such as SAP can reduce the size of live databases by as much as 80 per cent, leading to significant performance improvements. Optimizing application databases through a regular archiving program helps enterprises to maintain fast application response times, minimize storage costs and complete system upgrades and database restores faster, with less downtime and associated business risk.

Data can also be archived from legacy applications as part of a decommissioning program. Once all useful data is removed from the original application it can be retired, allowing the business to make savings against software, maintenance and infrastructure costs and to refocus resources on business growth initiatives.

CASE STUDY

The value of data disguising in system testing

A global logistics provider needed large volumes of realistic sample data for internal testing of its systems following a major software upgrade. The company lacked the facility to generate the required volumes of data, either in house or through its technology partners. Clearly, it was not acceptable for the company to use copies of real customer documents or data.

Anonymous data was required which followed the same patterns as actual customer information. To minimize exposure of customer data it was also important that IT staff should not need to work with production data files.

The company used the data disguising function in Columbus to replace text and numbers from the original files with random characters of the same type. The anonymization process is automated, enabling large volumes of suitable data to be created quickly, without intervention from the IT team.

Learn more

Bring us your information governance challenges and we will be happy to offer advice without obligation.

Contact us at market@macro4.com or call +44 1293 872 000 to speak to an expert.

MACRO 4
A Division of UNICOM Global

Macro 4 Headquarters
The Orangery
Turners Hill Road
Worth, Crawley
West Sussex
RH10 4SS
United Kingdom

Tel: +44 1293 872000
Email: market@macro4.com
www.macro4.com

Belgium
Tel: +32 15 74 74 80
Email: market.be@macro4.com

France
Tel: +33 1 79 71 84 50
Email: market.fr@macro4.com

Germany
Tel: +49 89 6100970
Email: market.de@macro4.com

Italy
Tel: +39 2 213 1941
Email: market.it@macro4.com

Netherlands
Tel: +39 20 5206874
Email: market.nl@macro4.com

Spain
Tel: +34 91 443 0220
Email: market.es@macro4.com

Switzerland
Tel: +41 44 723 40 00
Email: market.ch@macro4.com

USA
Tel: +1 973 526 3900
Email: market.usa@macro4.com

About Macro 4

Macro 4, a division of UNICOM Global, develops software solutions that accelerate business transformation. Macro 4's cross-platform enterprise information management solutions make it easy for companies to go digital, personalize customer communications and unlock the value of their corporate content. Macro 4 solutions for application lifecycle management, session management and performance optimization are used by many of the world's largest enterprises to modernize their mainframe applications and development processes. UNICOM Global operates across all geographic regions and offers deep in-house resources and flexible IT solutions to customers worldwide.

For more information on Macro 4 products and services visit www.macro4.com.

UNICOM® Systems, Inc.
UNICOM Plaza Suite 310, 15535 San Fernando Mission Blvd., Mission Hills, CA. 91345 USA
Tel: +1 818 838 0606 Fax: +1 818 838 0776 www.unicomglobal.com