WHITE PAPER

MACRO|4
A Division of UNICOM® Global

# COLUMBUS FÜR INFORMATION GOVERNANCE

Nutzen Sie Compliance zu Ihrem Vorteil

www.macro4.com

# Inhaltsverzeichnis

HERAUSFORDERUNGEN DER INFORMATION GOVERNANCE ..... 3
Die Rolle von EIM für die Information Governance .....4
Lösungen für Information Governance .....4

VORSCHRIFTEN ÄNDERN SICH PERMAMENT.....6
Lösungen zur Einhaltung von Vorschriften ..... 6

BLOCKCHAIN: ENE LÖSUNG FÜR COMPLIANCE ..... 9
Blockchain-fähiges EIM ..... 9

GDPR und CCPA: HOHE MESSLATTE FÜR DEN DATENSCHUTZ..... 11
Lösungen für den Datenschutz .....12

DIE ROLLE DER ARCHIVIERUNG FÜR INFORMATION GOVERNANCE .....14
Archivierungslösung der nächsten Generation .....14

WEITERE INFORMATIONEN..... 15

# Herausforderungen im Rahmen der Information Governance - heute und über 2022 hinaus

**Eine solide Information Governance ist Merkmal eines gut geführten Unternehmens. Doch die damit verbundenen Herausforderungen und Risiken sind größer als je zuvor.**

Die anhaltenden Auswirkungen von Datenverstößen bei Marriott und Equifax sowie der Skandal um Datenmissbrauch bei Facebook/Cambridge Analytica machen deutlich, dass Führungskräfte und Wirtschaft Information Governance ernst nehmen sollten.

Denn es geht dabei um weit mehr als nur um die Verwaltung von Informationen oder die Einhaltung von Vorschriften. Entscheidend ist, dass Unternehmen eine Strategie entwickeln, um Informationen zu schützen und sie verantwortungsvoll zu nutzen, um so Kundenvertrauen aufzubauen. Information Governance ist eine Disziplin, bei der Mitarbeiter auf allen Ebenen konsistente Richtlinien und Prozesse befolgen müssen, um angesichts unterschiedlicher - manchmal widersprüchlicher - Anforderungen von Kunden, Regulierungsbehörden, Gesetzgebern und internen Interessengruppen bewährte Verfahren aufrechtzuerhalten.

Cybersicherheit ist die Grundlage auf der alle anderen Maßnahmen der Information Governance aufbauen. Sie stellt auch 2022 die größte Herausforderung dar. Unternehmen rund um den Globus müssen auf kriminelle Bedrohungen reagieren, deren Ziel es ist, IT-Systeme zu infiltrieren und Unternehmensdaten zu stehlen oder zu manipulieren.

Auch neue Datenschutzgesetze erfordern Maßnahmen. Die Datenschutzverordnung der EU (DSGVO) hat seit ihrer Einführung im Mai 2018 einen großen Wandel in der Datenschutzpraxis bewirkt. Der kalifornische Consumer Privacy Act (CCPA) trat 2020 in Kraft, und mehrere andere US-Datenschutzgesetze werden in den nächsten 18 Monaten folgen, darunter der kalifornische Privacy Rights Act (CPRA) und der Colorado Privacy Act (CPA). Weltweit führen Regierungen strengere Datenschutzgesetze ein, die eine bessere Durchsetzung und hohe Geldstrafen bei Verstößen vorsehen. Darüber hinaus nehmen branchenspezifische Regulierungen zu. All dies stellt Unternehmen vor große Herausforderungen. Sie müssen die Einhaltung diverser Bestimmungen an allen Fronten sicherstellen. Dies geht nur, indem sie Prozesse und Systeme optimieren, die dem Compliance-Management, der Überwachung und dem Reporting dienen.

# Die Rolle von EIM für die Information Governance

**Systeme für Enterprise Information Management (EIM) sind immens wichtig für die Steuerung und das Management großer Datenströme, die durch ein Unternehmen fließen. EIM-Systeme sind Bestandteil der Unternehmensstrategie für Information Governance.**

EIM-Systeme sind so konzipiert, dass sie Informationen jedes Volumens verwalten können: eine wesentliche Anforderung, da das Datenwachstum weiterhin explosionsartig ansteigt. Nach Angaben des Marktforschungsunternehmens IDC[1] wird die weltweite Datenmenge jährlich um 61 Prozent wachsen und bis 2025 175 Zettabyte erreichen - das entspricht dem Volumen von 12,5 Milliarden der heute größten verfügbaren Festplatten. Laut IDC[2] werden 80 Prozent dieser Informationen unstrukturiert sein. Hier kommt das EIM-System ins Spiel.

### Unstrukturierte Daten “ordnen”

Unstrukturierte Daten stellen eine besondere Herausforderung dar, weil sie im Gegensatz zu den Daten aus traditionellen Datenbanken nicht logisch strukturiert sind - wie der Name schon sagt. Unstrukturierte Daten liegen in unterschiedlichsten Formaten und Layouts und an diversen Standorte vor, was die Kontrolle erheblich erschwert.

EIM bringt Ordnung in das vermeintliche Chaos, das durch diese ungeordneten, unstrukturierten Daten verursacht wird. Informationen werden automatisch erfasst, klassifiziert und verarbeitet, unabhängig von ihrem Format oder ihrer Herkunft. Das reicht von Dokumenten über Bildern und Videos bis hin zu Sprachaufzeichnungen, Chat-Protokollen, SMS-Nachrichten und Datensätzen aus Geschäftsanwendungen. Eine Automatisierung basierend auf Geschäftsregeln minimiert Kosten sowie manuellen Aufwand und verringert die Häufigkeit menschlicher Fehler, welche zur Verletzungen der Compliance führen können.

# Lösungen für Information Governance

**Columbus von Macro 4 ist eine hochskalierbare Lösung für Enterprise Information Management, die Content Services, Workflow, vorschriftsmäßige Datenspeicherung und Multi-Channel-Delivery beinhaltet.**

Unternehmen auf der ganzen Welt nutzen Columbus, um ihre unstrukturierten Daten zu organisieren, Information Management Tasks zu automatisieren und Kosten, Risiken und Aufwand für Information Governance zu reduzieren. Workflows gewährleisten, dass die richtigen Informationen der richtigen Person, am richtigen Ort, zur richtigen Zeit zur Verfügung stehen. Verschlüsselung, Manipulationssicherheit, Identitätsmanagement und Datentrennung sorgen für Datensicherheit in jeder Phase.

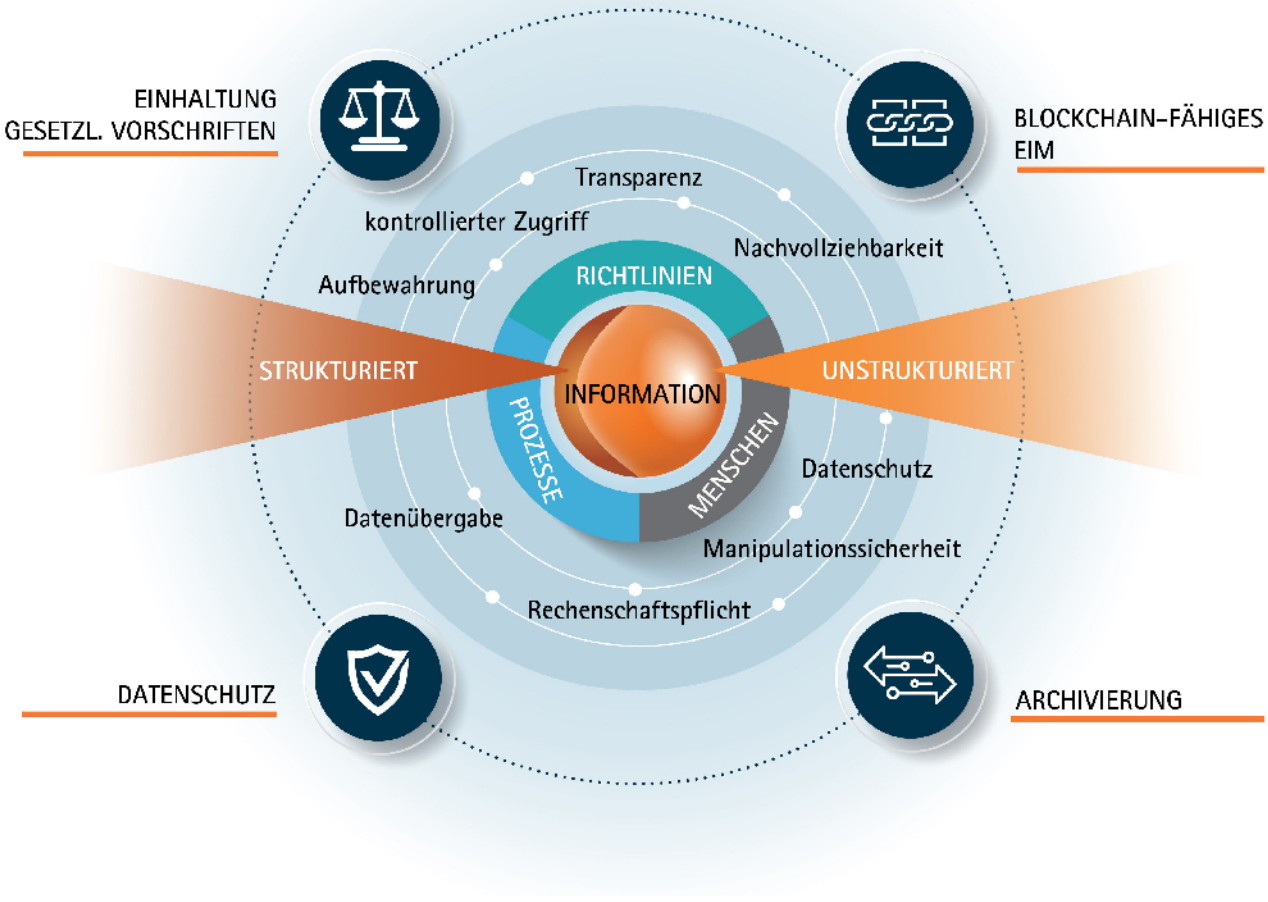
[1] IDC: Data Age 2025, The Digitization of the World from Edge to Core, 2018

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

Mit Unterstützung von Columbus setzen Unternehmen hochwirksame und beständige Praktiken für das Information Management sicher um und bauen so Vertrauen und Kundentreue auf. Denn die Verbraucher von heute sind sehr versiert, wenn es um den Schutz ihrer persönlichen Daten geht. Deshalb ist der verantwortungsvolle Umgang damit ein wichtiger Wettbewerbsfaktor.

Macro 4 stellt seit 20 Jahren erfolgreich Lösungen für Information Management bereit - über alle wichtigen Compliance-Bereiche und die unterschiedlichsten Branchen hinweg. Macro 4 bietet individuelle Lösungen, die von Professional-Services-Spezialisten genau auf die besonderen Herausforderungen jeden Unternehmens zugeschnitten werden. Darüber hinaus bietet der Hersteller spezialisierte Lösungen für die Einhaltung gesetzlicher Vorschriften, Blockchain-fähiges EIM, Datenschutz und Archivierung an.

## INFORMATION GOVERNANCE IN AKTION



# VORSCHRIFTEN ÄNDERN SICH PERMANENT

**Regulatorische Änderungen sind heute die Norm. Keine Branche bleibt von den wachsenden Anforderungen der organisatorischen Rechenschaftspflicht, Transparenz und Kontrolle verschont.**

Um Datenschutzbestimmungen einzuhalten, müssen Unternehmen strenge Regeln für die Verwendung von Kunden- und Mitarbeiterdaten befolgen. Dazu gehört es, einen hohen Sicherheitsstandards zu gewährleisten, sensible Inhalte zu schützen und Privatpersonen auf Anfrage Einsicht zu gewähren oder Daten zu löschen. Zusätzlich gibt es Hunderte von Branchen- und Länder-spezifischen Vorschriften zur Wahrung von Rechenschaftspflicht, Fairness und Transparenz bei geschäftlichen Transaktionen.

**Die meisten Regularien fordern:**

- Überwachung der Compliance und Aufdeckung von Verstößen
- Auditierung von Compliance-Prozessen und behördliche Berichterstattung
- Beweissicherung durch Archivierung, Maßnahmen zur Unveränderlichkeit und Rechtssicherheit

## Lösungen zur Einhaltung von Vorschriften

**Die Columbus-Suite bietet Information Lifecycle Management und Archivierung um Informationen zu erstellen, klassifizieren, verwenden, aufzubewahren oder zu vernichten. Alles im Einklang mit Ihren Compliance-Verpflichtungen.**

Dokumente und andere relevante Informationen werden gesichert, um als manipulationssichere Beweise für Geschäftsvorgänge und Transaktionen zu dienen. Aus Compliance-Gründen liegen Inhalte in einer Vielzahl von Formaten vor.  So können EU-konforme PDF- und/oder XML-Rechnungen erstellt werden, um den Standards ZUGFeRD, XRechnung und Factur-X zu entsprechen. Und Elemente können als “Legal Hold” gekennzeichnet werden, um so eine weitere Bearbeitung während Rechtsstreitigkeiten zu unterbinden.

Columbus eignet sich bestens für den Einsatz in hochsensiblen Sicherheitsbereichen wie der Strafverfolgung. Hier dient es dazu, die chronologische Dokumentation digitaler Beweise zu sichern wie z. B. polizeilicher Aufnahmen mit Körperkameras. Alle Aktivitäten im Zusammenhang mit einer Information - z. B. wie sie verarbeitet, wie auf sie zugegriffen oder wie sie verteilt wurde - werden in einem sicheren Audit-Trail aufgezeichnet. Dabei wird eine Blockchain-fähige Verschlüsselung verwendet, um Manipulationen zu verhindern (siehe auch Kapitel “Blockchain-fähiges EIM”).

Dokumenten-Workflows werden zentral verwaltet und überwacht. Automatisierte Warnmeldungen informieren sofort über nicht konforme oder verdächtige Systemaktivitäten und eine umfassende Berichterstattung steht bereit, welche den Anforderungen von Regulierungsbehörden und Stakeholdern gerecht wird. Geschäftsprozesse lassen sich durch Workflows abbilden und schnell an gesetzliche Änderungen oder neue Branchenvorschriften anpassen.

## Columbus: Funktionen für Datensicherheit und Datenschutz

Granulare Sicherheits- und Zugriffskontrollen bieten ein Höchstmaß an Schutz für Geschäftsinformationen. Datenschutzfunktionen schützen sensible und persönliche Daten.

- **Identity und Access Management (IAM)**
  Columbus unterstützt eine starke Benutzerauthentifizierung und lässt sich in IAM-Systeme von Drittanbietern integrieren, um Multi-Faktor-Authentifizierung (MFA), Biometrie, digitale Signaturen und Standortbestimmung zu ermöglichen. Zugriffsrechte können bis hinunter zur individuellen Feldebene gesteuert werden.

- **Datentrennung**
  Aus Gründen der physischen Sicherheit oder zur Einhaltung von Vorschriften, lassen sich Daten an mehreren physischen Orten und auf einer Vielzahl von Speichermedien speichern. Der Zugriff darauf wird zentral gesteuert.

- **Sichere Speicherung**
  Columbus speichert Daten sicher, manipulationsgeschützt und verschlüsselt auf manipulationssicherer Hardware; Blockchain-fähige Verschlüsselung und Prüfmechanismen gewährleisten die Unveränderbarkeit der Daten.

- **Schwärzen personenbezogener Daten**
  Daten können zum Zeitpunkt der Anzeige selektiv zensiert werden, um die Offenlegung persönlicher Informationen zu verhindern.

- **Datenanonymisierung**
  Zum Schutz der individuellen Vertraulichkeit, zum Beispiel bei der Verwendung persönlicher Informationen für statistische Zwecke, lassen sich Daten entweder vollständig anonymisieren oder alternativ pseudonymisieren. Die Pseudonymisierung ermöglicht Organisationen, Namen und andere persönliche Identifikatoren durch ein nicht zu identifizierendes Äquivalent wie z. B. einen Code zu ersetzen, der durch Verlinkung auf das Individuum zurückverweisen kann.

### Außerbetriebnahme von alten Speichersystemen

Alte Speichermedien verfügen oft nicht über die notwendigen Sicherheits- und Datenschutzfunktionen, um Geschäftsdaten angemessen zu schützen und die heutigen Standards der Information Governance zu erfüllen. Daten aus diesen Repositories können schnell nach Columbus migriert werden, und das Alt-System wird anschließend stillgelegt. Dies gewährleistet Compliance im Datenschutz und bietet die nötige Flexibilität für künftige Compliance-Anforderungen. Durch die Reduzierung der Anzahl von Content-Management-Systemen lassen sich zudem Kosten verringern.

## Bearbeiten sensibler Kundendaten im Open-Banking-Bereich

Anwenderbeispiel

Als Teil der Open-Banking-Initiative suchte ein großer britischer Finanzdienstleister einen Weg, um Daten von Privatkunden mit anderen regulierten Anbietern unter Einhaltung aller regulatorischen Standards auszutauschen.

Um den Payment Card Industry Data Security Standard (PCI DSS) bei der Weitergabe von Informationen im Namen ihrer Kunden einzuhalten, musste die Bank sensible Kredit- und Debitkartendaten, wie die primäre Kontonummer (PAN), aus ihren Dateien entfernen.

**Die Bank nutzte hierfür die Schwärzungsfunktion in Columbus und ersetzte die sensiblen Daten durch Black Boxes. Dies war eine sehr einfache Lösung, die selektiv und automatisch auf der Grundlage von Geschäftsregeln angewendet werden konnte. Dadurch musste die Bank keine Änderungen an ihren Kernsystemen vornehmen und keinen Drittanbieter beschäftigen, um das Layout ihrer elektronischen Dokumente zu ändern.**

# BLOCKCHAIN: EINE LÖSUNG FÜR COMPLIANCE

**Blockchain-Technologie spielt durch die Unveränderlichkeit von Daten eine große Rolle in der Compliance. Sind die Daten einmal in der Blockchain gespeichert, ist es praktisch unmöglich, sie zu ändern oder zu löschen. Wichtige Transaktionen, Dokumente und Aktionen können in die Blockchain geschrieben werden, um eine revisionssichere Aufzeichnung zu erhalten.**

Blockchain-Netzwerke sind auch für das Echzeit-Reporting im Rahmen von Compliance nützlich. Dadurch wird die Notwendigkeit der manuellen Datenerfassung verringert und die regulatorische Berichterstattung für Unternehmen und Aufsichtsbehörden gleichermaßen erleichtert.

Darüber hinaus unterstützen Blockchain-Netzwerke schnellere Identitätsprüfungen und verringern die Wartezeit für Kunden beim KYC-Verfahren (know your customer) und in Anti-Geldwäsche-Prozessen (AML). Denn sie ermöglichen es mehreren Parteien - wie Banken und ihren Kunden - Daten gemeinsam zu nutzen und zu validieren.

Trotz des wachsenden Interesses an der Blockchain für die Einhaltung von Vorschriften, bleiben führende Unternehmen bei neuen Investitionen zurückhaltend. Organisationen, die in regulierten Industrien tätig sind, suchen nach Möglichkeiten, Blockchain-Netzwerke für Compliance zu nutzen, ohne wesentliche Änderungen an ihrer bestehenden IT-Infrastruktur vornehmen zu müssen.

**Columbus bietet diese Möglichkeiten.**

## Blockchain-fähiges EIM

### Columbus: Das erste Blockchain-fähige Enterprise Information Management System

Columbus verwendet die gleichen Verschlüsselungsmechanismen wie Blockchain, um Daten zu erfassen und manipulationssicher aufzuzeichnen. Das gewährleistet die Unveränderbarkeit der im Columbus-Repository gespeicherten Informationen und weist nach, wie diese Informationen von wem und wann verwendet wurden.

Darüber hinaus lässt sich die Columbus-Suite in das Hyperledger-Blockchain-Framework integrieren, um eine zweite unveränderliche Version zu erstellen - mit allen Merkmalen, welche die verteilte Ledger-Technologie bietet. Dieser Ansatz ermöglicht es, praktisch unbegrenzt Daten auszutauschen - sei es mit Blockchain-Netzwerken, Regulierungsbehörden, Wirtschaftsprüfern, Kunden oder anderen Parteien von Regulierungsprozessen. Organisationen können den vollen Nachweis erbringen, dass die Compliance eingehalten wurde - wie z. B. die Verhinderung von unberechtigtem Zugriff oder das Löschen persönlicher Daten auf Anfrage.

## Eine Blockchain-Lösung für das “Recht auf Vergessen”

Fallbeispiel

Das Recht auf “Daten-Löschung” - bekannt als “Recht, vergessen zu werden” (DSGVO) und “Recht auf Löschung” (CCPA) - stellt Compliance-Spezialisten vor ein Rätsel. Wie liefert man einen schlüssigen Nachweis dafür, dass die Daten eines Kunden gelöscht wurden, ohne eine Dokumentation zu speichern, die auf den Kunden zurück verweist?

**Das folgende Beispiel aus dem Bankensektor veranschaulicht, wie mit der Blockchain-Technologie genau dieser Nachweis erbracht werden kann, ohne Spuren der persönlichen Daten des Kunden zu hinterlassen.**

Zunächst erstellt die Bank in ihrem Case Management System eine Fall-ID für die Anfrage und teilt diese dem Kunden mit. Die Daten des Kunden werden dann gelöscht und ein Audit-Trail wird in das Blockchain-Netzwerk geschrieben. In diesem sind alle Schritte dokumentiert, welche die Bank unternommen hat, um die Daten aus ihren Systemen zu löschen. Dieser Audit-Trail ist mit derselben Fall-ID verknüpft. Anschließend benachrichtigt die Bank den Kunden, dass der Fall abgeschlossen ist und vernichtet alle verbliebenen Daten des Falls (einschließlich der Fall-ID).

Ab diesem Zeitpunkt kennt nur noch der Kunde die Fall-ID. Er könnte später die Blockchain unter Verwendung der Fall-ID abfragen und das Audit-Protokoll einsehen, oder eine Aufsichtsbehörde damit beauftragen. Auf diese Weise wird die Integrität des Löschvorgangs gewahrt, während gleichzeitig Überprüfungen ermöglicht werden, die bestätigen, dass die Löschanfrage erfolgreich abgeschlossen wurde.

# DSGVO UND CCPA: HOHE MESSLATTE FÜR DEN DATENSCHUTZ

Die DSGVO regelt, wie Organisationen weltweit die persönlichen Daten von EU-Bürgern sammeln, speichern und nutzen dürfen. Sie wurde 2018 von der Europäischen Union eingeführt. Die DSGVO ersetzt die Datenschutzrichtlinie von 1995 und hat strenge, neue Datenschutzbestimmungen und hohe finanzielle Strafen bei Verstößen eingeführt. Unternehmen müssen mit Geldstrafen von bis zu 20 Millionen Euro oder vier Prozent ihres weltweiten Vorjahresumsatzes rechnen, je nachdem was höher ist.

CCPA gilt “nur” für Unternehmen, die in Kalifornien tätig sind und mit den Daten von in Kalifornien ansässigen Personen umgehen. Die Auswirkungen werden jedoch weltweit zu spüren sein, da Kalifornien die fünftgrößte Volkswirtschaft der Welt ist. CCPA ähnelt in vielerlei Hinsicht der DSGVO, legt jedoch einen besonderen Schwerpunkt auf die Einschränkung des Verkaufs von persönlichen Daten. Die Bußgelder sind im Vergleich zur DSGVO gering (bis zu $7.500 für einen vorsätzlichen Verstoß). Verbraucher können aber bis zu $750 pro Vorfall einklagen. Im Falle einer groß angelegten Verletzung der Privatsphäre könnte sich dies auf mehrere Millionen Dollar belaufen.

DSGVO wie CCPA stärken die Rechte des Einzelnen und verpflichten Organisationen zum Datenschutz, die personenbezogene Daten verarbeiten. Dies schließt Transparenz bei der Verwendung und schnelle Reaktion auf Kundenanfragen bezüglich Weitergabe oder Löschung ein (innerhalb eines Monats laut DSGVO, innerhalb von 45 Tagen laut CCPA). Außerdem soll eine Nutzung, welcher der Kunde bereits widersprochen hat oder die nicht im Einklang mit den Vorschriften steht, verhindert werden. Kommende weltweite Datenschutzgesetze werden voraussichtlich ähnliche Ansätze verfolgen.

### Strafen für EU-Datenschutzverletzungen: Die Auswirkungen

Beinahe täglich werden Bußgelder im Rahmen der DSGVO verhängt. Die drei größten bisher verhängten Strafen belaufen sich auf insgesamt 1 Milliarde Euro. Die Auswirkungen auf das Markenimage eines Unternehmens können sogar noch verheerender als das Bußgeld sein. Eine Organisation braucht unter Umständen Jahre, um das Vertrauen der Öffentlichkeit wieder zurückzugewinnen.

Verstöße gegen die DSGVO sind sehr unterschiedlich. Sie umfassen die Verletzung von Persönlichkeitsrechten, den Verlust von Computern oder die unsichere physische Speicherung sensibler persönlicher Daten. Artikel 32 bezieht sich ausdrücklich auf “unzureichende technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit”. Verstöße dagegen machen über 70 Prozent aller bisher verhängten Bußgelder aus.

EIM-Lösungen von Columbus unterstützen Organisationen bei der Einhaltung dieser Bestimmungen, durch eine zentrale Datenhaltung, fortschrittliche Datenschutz- und Sicherheitsmaßnahmen, starke Authentifizierung, manipulationssichere Speicherung und Datenschwärzung.

# Lösungen für den Datenschutz

**Das Management riesiger Mengen unterschiedlichster Kundendaten in Übereinstimmung mit strengen Datenschutz-Regeln ist eine ständige Herausforderung. Columbus ermöglicht Unternehmen, jegliche Form von Unternehmensdaten zu verwalten, verarbeiten und zu speichern - im Einklang mit der DSGVO und dem CCPA. Columbus lässt sich an neue Regulatorien jederzeit einfach und flexibel anpassen.**

## Datenzugriff, -übertragung und -löschung managen

Eine von Macro 4 durchgeführte Studie hat gezeigt, dass Organisationen Schwierigkeiten haben, Kunden den gewünschten Zugriff auf ihre persönlichen Daten zu gewähren. So werden z. B. Fristen nicht eingehalten oder Informationen unvollständig, schlecht formatiert oder kaum verständlich geliefert. Solche Compliance-Verletzungen sind häufig eine Folge davon, dass persönliche Informationen aus einer Vielzahl von Systemen und Formaten zusammengestellt werden müssen.

Die Columbus-Suite hilft Unternehmen, Informationen besser zu klassifizieren, zusammen zu stellen und zu formatieren, so dass sie schnell und effektiv Antworten liefern können, wenn ein Kunde seine Daten einsehen, zu einem anderen Anbieter übertragen oder löschen lassen möchte. Daten lassen sich automatisiert klassifizieren, so dass sie besser durchsuchbar sind. Eine Vielzahl von Klassifizierungskriterien wie Dateneigentümer, Inhaltstyp, Sicherheitsstufe oder erforderliche Aufbewahrungsfrist lässt sich festlegen. Darüber hinaus ermöglicht die Integration mit Analyse-Tools, dass persönliche Informationen aus unstrukturierten Daten heraus klassifiziert werden können.

Sowohl die DSGVO als auch der CCPA verlangen von den Unternehmen die Bereitstellung von Daten in tragbaren Formaten zu einfachen Weitergabe an Dritte. Columbus erleichtert diesen Prozess durch die Umwandlung von Daten aus verschiedenen Quellen in gängige Formate wie PDF, CSV und XML.

Regeln für den Lebenszyklus von Informationen stellen sicher, dass Kundenanfragen für Zugriff, Löschung oder Übertragung automatisiert ausgeführt werden, sofern dies nicht anderen gesetzlichen Bestimmungen widerspricht.

### Compliance Monitoring, Auditierung und Reporting

Columbus bietet eine proaktive Echtzeit-Überwachung aller Aktivitäten im Zusammenhang mit persönlichen Daten, wie z. B. Zugriff, Verarbeitung und Löschung. Es kann potenzielle Probleme bei der Einhaltung von Vorschriften sowie verdächtige Aktivitäten nachweisen, wie zum Beispiel ungewöhnliche Zugriffsversuche auf SIEM-Systeme (Security Information and Event Management). Informationen können mit Regulierungsbehörden und Wirtschaftsprüfern auf Blockchain-Plattformen ausgetauscht werden, um den Nachweis der Konformität zu erbringen.

### Datenschutz by Design and by Default: für die DSGVO unerlässlich

Organisationen sind verpflichtet, Technologien und Prozesse einzuführen, um die DSGVO-Datenschutzprinzipien zu befolgen und die Rechte des Einzelnen zu schützen. Diese Anforderungen, die als “Data Protection by Design and by Default” bekannt sind, werden durch Maßnahmen zur Datensicherheit und zum Schutz der Privatsphäre erfüllt, die in die Columbus-Suite integriert sind und die personenbezogene Daten langfristig schützen.

### Datenminimierung und Aufbewahrungsmanagement

Nach der DSGVO dürfen Unternehmen nur zwingend benötigte personenbezogene Daten und diese nur so lange wie unbedingt nötig aufbewahren. Columbus ermöglicht es, Richtlinien für die Datenaufbewahrung festzulegen, um diese “von der Wiege bis zur Bahre” zu verwalten und fristgerecht zu löschen - sowohl automatisch als auch auf Anfrage.

Die wichtigsten Ergebnisse der britischen Studie von Macro 4, wie Unternehmen Kundenanfragen auf Zugang zu ihren persönlichen Daten behandeln:

**32%**
**Nicht compliant mit Vorschriften der DSGVO**

**59%**
**Kundenservice unsicher, wie damit umzugehen ist**

**49%**
**Wiederholte Kundennachfrage zur Erfüllung nötig**

**59%**
**Nicht in der Lage, Daten elektronisch an den Kunden zu senden**

# DIE ROLLE DER ARCHIVIERUNG IM INFORMATION GOVERNANCE

**Die langfristige Aufbewahrung von strukturierten und unstrukturierten Daten ist eine entscheidende Komponente der Unternehmensführung und der Compliance.**

Um gesetzliche und behördliche Anforderungen zu erfüllen, sind Informationen wie historische Finanzunterlagen, Verträge und andere rechtliche Dokumente unter Umständen mehrere Jahre lang aufzubewahren; bestimmte Datenkategorien müssen während der gesamten Lebensdauer des Kunden oder sogar unbegrenzt aufbewahrt werden.

Historische Aufzeichnungen können für die Bearbeitung von Kundenanfragen oder für betriebliche Aktivitäten erforderlich sein. In diesem Zusammenhang wird die Integration von Archiven mit Geschäftsanwendungen empfohlen, um einen schnellen Zugriff zu ermöglichen.

Die Archivierung hat auch eine technische Dimension. Das Vorhalten historischer Daten in stark genutzten Geschäftsanwendungen kann Performance-Probleme verursachen, die durch die Archivierung älterer oder redundanter Daten behoben werden können.

## Archivierungslösung der nächsten Generation

**Der Ansatz von Macro 4 besteht darin, ein “lebendes” Archiv zu schaffen, auf das Business- und IT-Teams im Tagesgeschäft leicht zugreifen können.**

Das gesamte Spektrum der Unternehmensdaten kann im Columbus-Repository archiviert werden, einschließlich Datenbankeinträge, Dokumente und unstrukturierte Daten. Alle archivierten Informationen werden in einem sicheren, unveränderbaren Format vorgehalten und bis zur Entsorgung am Ende der Lebensdauer im Einklang mit den Unternehmensrichtlinien regelkonform verwaltet. Die Daten werden komprimiert, wodurch Milliarden von Daten gesichert und von einem einzigen Server aus zugänglich gemacht werden können.

Columbus lässt sich in Geschäftsanwendungen integrieren, um einen nahtlosen Benutzerzugriff auf archivierte Daten zu ermöglichen. Das Archiv stellt umfassende Geschäftsdaten bereit, die mit Hilfe von Business-Intelligence-Plattformen analysiert werden können.

Die Archivierung von Daten aus Inhouse-Systemen oder Anwendungen von Drittanbietern wie SAP® kann die Größe von Live-Datenbanken um bis zu 80 Prozent reduzieren und zu erheblichen Leistungsverbesserungen führen.

Dies hilft Unternehmen, Reaktionszeiten von Anwendungen zu verkürzen, Speicherkosten zu reduzieren, System-Upgrades und Datenbankwiederherstellungen schneller durchzuführen sowie Ausfallzeiten und damit verbundene Geschäftsrisiken zu minimieren.

Im Rahmen eines Programms zur Außerbetriebnahme können auch Daten aus Altanwendungen archiviert werden. Sobald alle relevanten Daten aus der Originalanwendung entfernt sind, kann diese ausgemustert werden. Dadurch erzielt das Unternehmen Einsparungen bei der Software, senkt Wartungs- sowie Infrastrukturkosten und kann Ressourcen auf Wachstumsinitiativen konzentrieren.

## Der Stellenwert der Datenverschleierung bei Systemtests

Anwenderbeispiel

Ein globaler Logistikanbieter benötigte große Mengen realistischer Testdaten für interne Systemtests nach einem größeren Software-Upgrade. Dem Unternehmen fehlte die Möglichkeit, die erforderlichen Datenmengen entweder intern oder über seine Technologiepartner zu erzeugen. Natürlich konnte das Unternehmen dafür keine Kopien von echten Kundendokumenten oder -daten verwenden.

Es wurden anonyme Daten benötigt, die dem gleichen Muster wie die tatsächlichen Kundeninformationen folgten. Um die echten Kundendaten zu schützen, war es auch wichtig, dass das IT-Personal nicht mit diesen arbeiten musste.

**Deshalb nutzte das Unternehmen die Datenverschleierungsfunktion in Columbus, um Text und Zahlen aus den Originaldateien durch zufällige Zeichen desselben Typs zu ersetzen. Der Anonymisierungsprozess ist dabei automatisiert, wodurch große Mengen geeigneter Daten schnell und ohne Eingreifen des IT-Teams erstellt werden können.**

# Erfahren Sie mehr darüber...

**Nennen Sie uns Ihre Herausforderungen im Bereich der Information Governance und wir beraten Sie gerne - natürlich ohne Verpflichtung.**

**Kontaktieren Sie unsere Experten unter market.de@macro4.com oder +49 89 6100970**

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
E-Mail: market@macro4.com
www.macro4.com

**Belgien**
Tel: +32 15 74 74 80
E-Mail: market.be@macro4.com

**Frankreich**
Tel: +33 1 79 71 84 50
E-Mail: market.fr@macro4.com

**Deutschland**
Tel: +49 89 6100970
E-Mail: market.de@macro4.com

**Italien**
Tel: +39 2 213 1941
E-Mail: market.it@macro4.com

**Niederlande**
Tel: +39 20 5206874
E-Mail: market.nl@macro4.com

**Spanien**
Tel: +34 91 443 0220
E-Mail: market.es@macro4.com

**Schweiz**
Tel: +41 44 723 40 00
E-Mail: market.ch@macro4.com

**USA**
Tel: +1 973 526 3900
E-Mail: market.usa@macro4.com

## Über Macro 4

Macro 4, ein Geschäftsbereich von UNICOM Global, entwickelt Softwarelösungen, welche die Transformation von Unternehmen beschleunigen. Die plattformübergreifenden Lösungen für Enterprise Information Management von Macro 4 erleichtern Unternehmen die digitale Transformation und Personalisierung ihrer Kundenkommunikation und steigern zudem den Nutzen ihrer Unternehmensdaten. Lösungen von Macro 4 für Application Lifecycle Management, Session Management und Performance-Optimierung werden von vielen der weltweit größten Unternehmen zur Modernisierung ihrer Mainframe-Anwendungen und Entwicklungsprozesse eingesetzt. UNICOM Global ist in allen geografischen Regionen tätig und bietet seinen Kunden weltweit fundiertes Know-How und flexible IT-Lösungen.

**Weitere Informationen zu den Produkten und Dienstleistungen von Macro 4 finden Sie unter 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