BCT Deutschland GmbH	
Titel	**DOK.magazin**
Ausgabe	2/2019, 14.05.2019
Seite	50-52
Auflage	7.500

Compliance 2.0: The Final Countdown

#Enterprise #Information #Management, #EIM, #Robotic-Process-Automation, #KI, #plattformbasierte #Geschäftsmodelle, #Datenschutz

Thomas Kuckelkorn ist als Manager PR & Kommunikation für die **BCT Deutschland GmbH** tätig. Mit seiner branchenübergreifenden Enterprise-Information-Management-Technologie sorgt BCT seit 1985 bei Nutzern für transparente, sichere und effiziente Informationsprozesse. Partner erweitern mit den EIM-Komponenten ihr vorhandenes Produkt- und Dienstleistungsportfolio oder entwickeln in Co-Creation mit BCT digitale und plattformbasierte Geschäftsmodelle. Seit 2010 ist das niederländische Unternehmen als BCT Deutschland in Aachen aktiv.

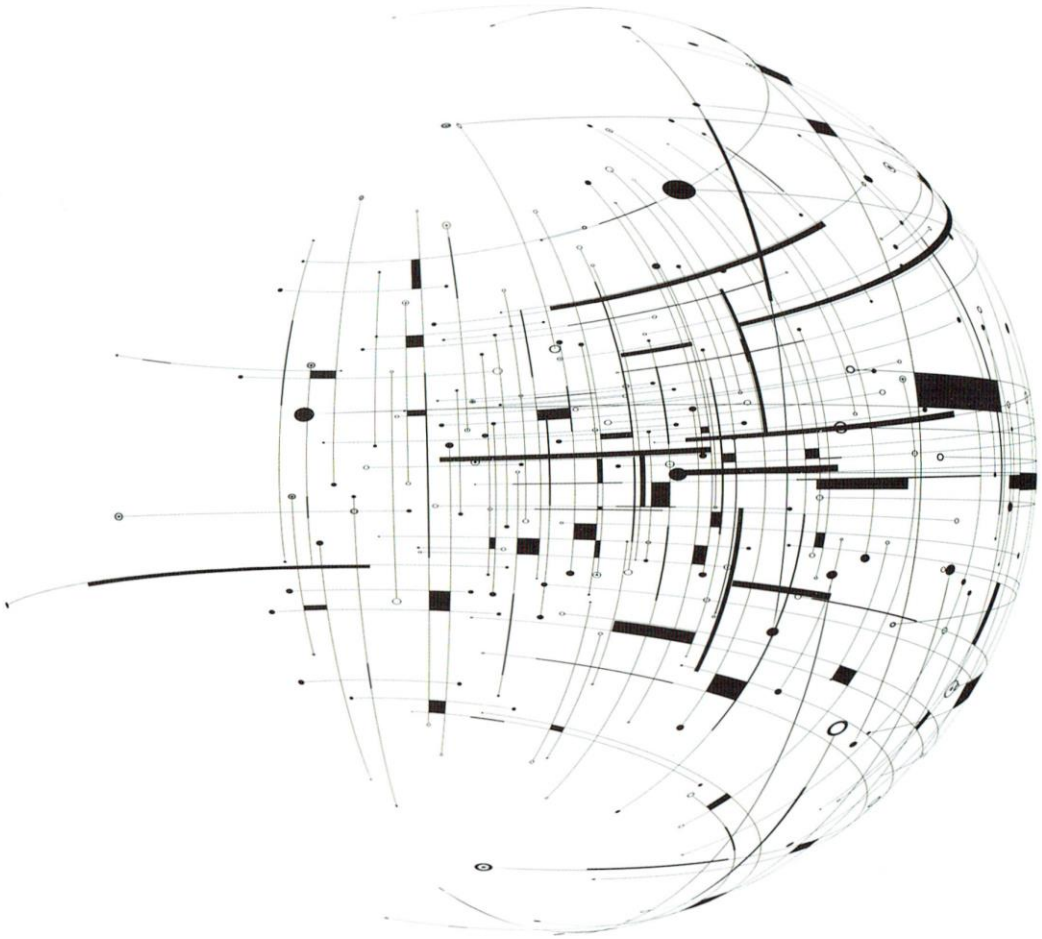
www.bctsoftware.com

Organisationen müssen sich zur Zeit intern wie extern auf neue Compliance-Vorschriften einstellen. Denn die Digitalisierung krempelt nach und nach auch bestehende Gesetze und Richtlinien um. Für Organisationen – darunter fallen Unternehmen, Behörden und Institutionen – bedeutet dies, die eigenen Compliance-Vorschriften kontinuierlich auf die neuen, digitalen Gegebenheiten anpassen zu müssen. Dabei gilt es vor allem Verantwortlichkeit und Nachweisbarkeit klar zu definieren – und dies auf verschiedenen Ebenen. Dazu müssen sich Organisationen mit wesentlichen Fragen auseinandersetzen.

Wer gewährleistet die Vollständigkeit der Daten?

Aktuell erhalten Technologien wie Robotic Process Automation (RPA) über die industrielle Anwendung hinaus Einzug in Bürolandschaften. Sie befreien Mitarbeiter von oftmals ungeliebten Standardaufgaben, da sie routinierte Tätigkeiten schnell und automatisiert übernehmen. Im Bereich des Input Managements wird die RPA-Software etwa für die Übertragung der Daten in Folgesysteme sowie die Einbindung in nachstehende Prozesse eingesetzt. Diese Technologie entlastet somit bei Aufgaben, die stets nach einem gleichen Raster auf Basis strukturierter Informationen erfolgen.

Eine Stufe weiter geht Artificial Intelligence (AI): Bei unstrukturierten Informationsabläufen greift die künstliche Intelligenz, indem sie selbstständig aus vergangenen Handlungen Rückschlüsse auf gegenwärtige Situationen zieht: „Tritt Fall X ein,



muss Reaktion Y folgen." Unabhängig von der Informationsstruktur greifen in einer dynamischen Echtzeitwelt auch objektbasierte Lösungen weiter als dokumentenorientierte Technologien. Denn der Informationsstand kann etwa über das Internet of Things kontinuierlich nachgehalten und verfolgt werden.

- Betrachtet man das Ganze unter dem Aspekt der Compliance, müssen darüber hinaus Mechanismen zur Verfügung stehen, die verhindern, dass autonom agierende Systeme relevante Daten löschen. Daher muss die Frage nach der diesbezüglichen Verantwortung geklärt werden.

Wer zeichnet verantwortlich für die Inhalte?

In einer digitalen Welt wächst das Angebot an plattformbasierten Geschäftsmodellen. Sie sind die Reaktion auf das veränderte Verhalten im Privaten: Man bestellt, bucht und beantragt online – will folglich auch digital arbeiten und kommunizieren. Im Hinblick auf Kunden sind die neuen Plattformen besonders serviceorientiert. Denn durch synchrones und dynamisches Arbeiten innerhalb der Organisation und der gesamten Werkschöpfungskette können Anfragen zeitnah bearbeitet werden und beispielsweise automatisierte Statusmeldungen geteilt werden.

Darüber hinaus verstehen sich Organisationen zunehmend als Teil eines großen Netzwerks. Sie können also als Partner an bestehende digitale Strukturen anknüpfen oder aber in Co-Creation sogar neue Services oder ganze Geschäftsmodelle entwickeln.

- Beantwortet werden muss in Bezug auf Compliance die Frage nach der Verantwortlichkeit, wenn Inhalte auf diese Plattformen hochgeladen werden, insbesondere wenn es sich dabei um Rechtsverstöße handelt.

Wer haftet für unberechtigte Zugriffe?

Immer mehr wird auch im Digital Workplace gearbeitet. Dadurch reagieren Arbeitgeber auf die Wünsche von Mitarbeitern, Aufgaben flexibler und selbstbestimmter erledigen zu können. Doch um smart arbeiten zu können, müssen Organisationen technische Grundlagen schaffen wie die Bereitstellung mobiler Endgeräte und eine sichere Verbindung zum organisationseigenen Server.

Für eine geschützte digitale Zusammenarbeit innerhalb der Organisation sowie mit Dritten muss auch der Smart Worker selbst für Sicherheit im Digital Workplace sorgen, unter anderem etwa durch eine Bildschirmsperre beim Verlassen des Arbeitsplatzes, aber auch durch den Schutz personenbezogener Daten. Wenn das mobile Arbeiten ohne festgelegte Regeln neu eingeführt wurde, sollten Mitarbeiter aktiv den Austausch mit Vorgesetzten suchen.

- Entscheidend für die Compliance ist der Aspekt, wer bei Datenverlust oder unberechtigten Zugriffen haftet – wenn beispielsweise Geräte beim mobilen Arbeiten gestohlen werden.

Wie werden rechtliche Bestimmungen umgesetzt?

Im Gegensatz zu den drei genannten Aspekten, die die Organisationen von innen heraus bestimmen, ist der Faktor Recht extern gesteuert. In Zeiten mobilen Arbeitens und eines Informationsaustauschs via Cloud ist ein Sicherheitsrahmen für Menschen und Daten essenziell. Gesetze wie die Datenschutzgrundverordnung (DSGVO) setzen neue rechtliche Standards und müssen auch aus Compliance-Sicht eingehalten werden. So wird beispielsweise auf Gesetzesebene die digitale Eingangsrechnungsverarbeitung in Form von Standards wie ZUGFeRD und XRechnung vorangetrieben: Bundesministerien und Verfassungsorgane sind bereits verpflichtet, Rechnungen nur noch in elektronischer Form zu empfangen und zu verarbeiten; weitere öffentliche Auftraggeber und sicherlich auch die restliche Organisationswelt sollen folgen. Bei Nichteinhaltung müssen Organisationen ihren Verstoß rechtfertigen und es kann zu Strafen, unter anderem in Form von Abmahnungen oder Bußgeldern, kommen.

- Rechtliche Vorgaben definieren somit Verantwortungen und ermöglichen eine Nachweisbarkeit bei Fehlverhalten. Wesentlich dabei ist, dass Organisationen interne Maßnahmen festlegen müssen, um geltende rechtliche Standards zu erfüllen.

Fazit

Ein Informationsmanagement-System ist ein effektives und sicheres Tool, um auf technologischer Ebene den gewandelten Nutzungsbedürfnissen von Mitarbeitern sowie dem neuen Serviceanspruch der Kunden gerecht zu werden. Compliance-Vorschriften, die sich in Zeiten digitaler Prozesse jedoch stetig ändern, definiert es hingegen nicht. Hier sind die Organisationen in der Pflicht, bestehende Richtlinien auf ihre Tauglichkeit sowie festgelegte Verantwortlichkeiten und Nachweispflichten kontinuierlich zu hinterfragen und neue festzusetzen. So vermeiden sie zuverlässig Compliance-Verstöße und sorgen für eine nachhaltige Organisationsführung.