



Herbert Loerch, General Manager EMEA bei Hyland: „Die Zukunftsfähigkeit des ECM-Systems in Unternehmen hängt davon ab, wie fern es die digitale Transformation unterstützt und ob es den hohen Anforderungen der DSGVO hinsichtlich der Rechtssicherheit entspricht.“

**Hyland: Ein brandgefährliches Datendickicht**

## ECM: jetzt sicher migrieren

Die nahende – oder vielleicht besser drohende – Datenschutzgrundverordnung (DSGVO) ist der ideale Zeitpunkt, um das ECM in Unternehmen zu modernisieren. Das schafft Rechtssicherheit und bringt zudem Vorteile in der Digitalisierung. Herbert Loerch von Hyland berichtet.

„Trotz der Brisanz, die die DSGVO mit sich bringt, sind Unternehmen in Deutschland auf den Stichtag im Mai 2018 noch nicht ausreichend vorbereitet“, berichten die Consultants der IDC (International Data Corporation). „44 Prozent der befragten Organisationen haben noch keine konkreten Maßnahmen zur Erfüllung der Anforderungen gestartet, darüber hinaus fehlt vielen immer noch der ganzheitliche Blick auf alle personenbezogenen Daten im Unternehmen.“

Oftmals herrscht in Organisationen der Irrglaube, dass lediglich die bekannten Stammdaten aus bereits bekannten Anwendungen unter die DSGVO fallen. Das ist fatal, denn aus technischer Sicht können auch schon eine archivierte Notiz im CRM („Herr Schmitz von XY bittet um Rückruf“) oder eine gespeicherte IP-Adresse personenbezogene Daten enthalten. Wenn sich Organisationen also weiterhin auf veraltete File-Systeme oder ECM der ersten Generation verlassen, lauern an vielen Stellen potenziell gefährliche Unwägbarkeiten – die Rechtssicherheit kann so nur schwer gewährleistet werden. Es ist also schon allein aus den juristischen Gründen der DSGVO wichtig, genau jetzt eine ganzheitliche ECM-Strategie zu starten.

Die IDC-Studie ergab weiterhin, dass 44 Prozent der befragten Unternehmen bisher noch keine Aktivitäten im Kontext der DSGVO angestoßen

haben: „Vorbereitungen werden nicht mit der erforderlichen Ernsthaftigkeit verfolgt und potenzielle Konsequenzen verharmlost“, so die Consultants. Das ist insbesondere hinsichtlich der ECM-Migration bedenklich, denn: „Rund ein Drittel der Unternehmen weiß nicht, wann personenbezogene Daten gelöscht werden müssen, welche Anwendungen die Daten verarbeiten und wer Zugriff auf die Daten hat“, so die Studie. Kurz gesagt: Es existiert ein Datendickicht, das aus rechtlichen Gründen brandgefährlich ist.

### ECM in Zeiten der Digitalisierung

Doch nicht nur diese Gefahr können Unternehmen durch die Migration ihrer ECM bannen. Vielmehr schlagen sie damit gleich zwei Fliegen mit einer Klappe: Sie können sich zum einen

hinsichtlich der DSGVO besser absichern, zum anderen die digitale Transformation im Unternehmen weiter vorantreiben, was mit On-Premise Legacy-Systemen schwierig, wenn nicht gar unmöglich ist. Es ist also mehr als hilfreich, das Thema Migration strategisch anzugehen und den Wandel konsolidiert umzusetzen.

ECM in Zeiten der Digitalisierung – das bedeutet vor allem eine massiv steigende Anzahl von Content-Quellen. Selbst wenn man die gigantischen Wachstumsraten von Daten aus IoT- und Industrie-4.0-Umgebungen außen vor lässt, kommen beinahe täglich neue Inhalte hinzu: interne Kommunikation, Blogs, Webseiten, Collaboration Tools und letztlich die Digitalisierung tradierter Applikationen wie etwa Rechnungsverarbeitung, Zahlungsabwicklung, Auftragsbearbeitung und Vertragsmanagement.

Dieses – man muss es so nennen – Flickwerk aus unterschiedlichsten Technologien in die Cloud und somit in das digitale Zeitalter zu überführen, ist nicht zeitgemäß. Die technologische

Mit der Migration Ihrer ECM können sich Firmen hinsichtlich der DSGVO besser absichern und die digitale Transformation weiter vorantreiben.

Legacy-ECM-System



Neues ECM-System



Dokumente

Daten

Prozesse

Basis des ECM sollte aus nachvollziehbaren Gründen deshalb aus einer einzigen Plattform bestehen. Unternehmen sind auch so schon mit der Konsolidierung von betrieblicher Basis-IT, also beispielsweise Finanzapplikationen, ERP und Produktionssystemen, demselben beschäftigt, dass sie andere Sorgen haben, als zur Integration einer neuen App ins ECM jedes Mal einen groß angelegten Programmieraufwand betreiben zu müssen. Laufend neue Skripte entwickeln, Schnittstellen prüfen oder neu anlegen und mehrfach einen neuen Loop programmieren, ist kein zielgerichtetes Vorgehen. Stattdessen gilt es, mithilfe von Templates, Workflows und Point-and-Click-Prozessen zu arbeiten – standardisierte Einfachheit ist hier der Schlüssel und wirkt extrem unterstützend.

### Mobilität nicht auf Kosten der Sicherheit

Selbstverständlich muss ein ECM zu einhundert Prozent Cloud-fähig sein, damit diese Transformation gelingt. Allein damit ist es jedoch nicht getan, denn in der Digitalisierung ändern sich auch Geschäftsprozesse, interne Abläufe sowie die Anbindung von Kunden und Partnern. Deshalb darf Folgendes nicht vergessen werden: Ein tragfähiges ECM ist ein mobiles ECM. Das bedeutet: Die Anbindung von Tablets oder Laptops sowie ein einfacher Zugriff auf relevante Inhalte von außen müssen stets möglich sein. Selbstverständlich darf diese Mobilität nicht auf Kosten der Sicherheit gehen. Entscheidend ist des Weiteren, das mobiles ECM nicht nur das Teilen und Anse-

hen von Content ermöglicht, sondern auch das aktive Arbeiten. Das heißt beispielsweise, dass Freigabeprozesse jederzeit möglich sein müssen – völlig unabhängig davon, ob der Verantwortliche im Büro sitzt oder gerade unterwegs ist. Der Workflow muss seinen Namen also alle Ehre machen; Medienbrüche dürfen kein Thema mehr sein.

Fazit: Die Zukunftsfähigkeit des ECM-Systems in Unternehmen hängt davon ab, inwiefern es die digitale Transformation unterstützt und ob es den hohen Anforderungen der DSGVO hinsichtlich der Rechtssicherheit entspricht. Hundertprozentige Migrationsfähigkeit, Mobilität, Cloud-Fähigkeit und der Umgang mit unterschiedlichsten Content-Quellen gehören in jedem Fall dazu. ([www.onbase.com](http://www.onbase.com))

## VdS: Richtlinien zur effizienten Umsetzung

### Praktikable Vorgaben

Jedes Unternehmen in der EU muss die neue Datenschutz-Grundverordnung zum 25. Mai 2018 erfüllt haben – wobei die gravierenden Anforderungen häufig zusätzlicher Interpretationen bedürfen. VdS, Europas größtes Institut für Unternehmenssicherheit, unterstützt speziell Mittelständler mit praktikablen Vorgaben zur konkreten Umsetzung der EU-Forderungen.

Die nächste erweiterte Anforderung vor allem für mittelständische Unternehmen, die personenbezogene Daten verarbeiten, ist inzwischen gesetzlich verankert: Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (DSGVO) in sämtlichen Mitgliedsländern in Kraft – mit gravierenden und oft vagen Forderungen, für deren Umsetzung bislang keine praktikable Standards existierten.

Jedes einzelne Unternehmen nicht nur in Deutschland muss zum 25. Mai die DSGVO einhalten. Die Auswirkungen dieser Verordnung auf

Organisation, Kundenmanagement und auch IT gerade von Mittelständlern sind teils so tiefgreifend, dass wir definitiv sagen müssen: Es bleibt nicht mehr viel Zeit“, betont Dr. Robert Reineremann, Sprecher der Geschäftsführung bei VdS, Europas größtem Institut für Unternehmenssicherheit:

„Wir nutzen unser Expertenwissen, um die betroffenen Parteien auch auf diesem Gebiet mit gewohnt praxisnahen Richtlinien zu unterstützen. Anhand der neuen VdS 10010 können gerade kleinere Unternehmen Datenschutz mit optimaler Mitteleffizienz umsetzen – und zwar so, dass alle Vorgaben der DSGVO eingehalten werden.“

Die nötige Praktikabilität und die präzise Ausrichtung an der unternehmerischen Realität sichert die aktuelle VdS-Publikation durch die Beteiligung zahlreicher Organisationsexperten und Datenschutzverantwortlicher direkt aus mittelständischen Firmen. Mit den kompakten Richtlinien stellen Verantwortliche die Einhaltung der DSGVO



VdS unterstützt die Firmen mit eigenen Richtlinien zur praktikablen Umsetzung der DSGVO und stellt diese kostenlos zur Verfügung.

in ihrem Unternehmen sicher – und dies auditierungs- und zertifizierungsfähig. Die Richtlinien VdS 10010 zum Datenschutz-Management sind eng verzahnt mit den prämierten VdS 3473 zur Informationssicherheit.

Die Hilfestellungen zur praxisnahen Umsetzung der EU-Vorgaben präsentierte VdS auf der IT-Security-Messe it-sa in Nürnberg (10.-12. Oktober) erstmals der Öffentlichkeit. Auf [vds.de/dsgvo](http://vds.de/dsgvo) stehen die Richtlinien kostenlos zur Verfügung. ([www.vds.de](http://www.vds.de))