Stammdaten sind das Basiswissen für die Prozesse eines jeden Unternehmens. Man stelle sich vor, man fährt nach einer veralteten oder falschen Karte. Selbst wenn man überhaupt sein Ziel erreicht, dann auf jeden Fall zu spät und mit erhöhten Reisekosten. Mit den Stammdaten ist es ähnlich. Dass ein effektives und gut durchdachtes Stammdatenmanagement auch wesentlich zur DSGVO-Compliance beiträgt ist mehr als nur ein positiver Nebeneffekt.

Master Data Management

Robin Höhl
IT Management Consultant (CTI Consulting GmbH)

Was sind Stammdaten eigentlich genau?

Stammdaten gelten als zentrale Geschäftsobjekte und differenzieren sich aufgrund ihrer statischen Eigenschaft von Bewegungsdaten, da sie selten im Verlauf eines Geschäftsprozesses geändert werden. Im Fall von Kundenstammdaten betrifft dies bspw. die Adresse des Kunden. Stammdaten haben aufgrund der Zugriffe von Geschäftsprozessen einen immateriellen Wert, der leider oft erst wahrgenommen wird, wenn die Qualität der Stammdaten unzureichend ist und daher Fehler unterlaufen.

Ein Beispiel zur Veranschaulichung:

Ein Kunde gibt eine Bestellung auf und bezahlt fristgerecht. Die Ware soll ihm zugeliefert werden, allerdings entspricht die Adresse aufgrund von Inkonsistenzen zwischen den Systemen nicht derjenigen, die beim Spediteur hinterlegt ist. Das Paket wird an die falsche Adresse geliefert und es entstehen Folgekosten.

Die aktuelle Situation:

Durch vertikal optimierte Applikationen (Best-of-Breed) neigen Unternehmen zu einer zunehmend heterogenen IT-Landschaft, die ein großes Potential für „Datensilos“ aufweist. Das damit einhergehende Resultat ist eine redundante Stammdatenhaltung, die zu Inkonsistenzen und fehlerhaften Daten führen kann.

Um dieser Problematik entgegenzuwirken, eignet sich eine integrierte und zentralisierte Art der Stammdatenhaltung: Das Master Data Management (Stammdatenverwaltung) unterstützt die konsistente und redundanzfreie Stammdatenhaltung, indem die Pflege und/oder Analyse in einem zentralisierten System durchgeführt wird.

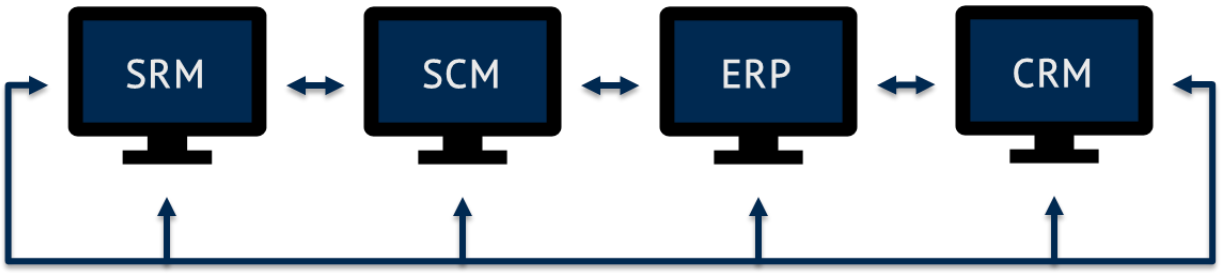

Abbildung 1: Standard-Systemintegration (Beispiel)

Die gängigen Methoden von MDM:

Registry Style:

Bei dem Registry Style werden Duplikate unter Zuhilfenahme von Bereinigungs- und Matching-Algorithmen aus diversen Quellsystemen entfernt werden. Darüber hinaus werden den übereinstimmenden Daten globale IDs zugeordnet und deshalb nicht als System of Record (SOR), sondern vielmehr als System of Reference angesehen werden kann.

Die Daten werden folglich nicht mit dem Quellsystem gespiegelt, sondern referenzieren als Konsolidierungs- und Korrekturhilfe der bereits existierenden Quellsysteme. Informationen für den Abgleich und die Verknüpfung der entsprechenden Datensätze werden gespeichert.

Für eine umfassende Sicht, die bspw. über einen Kunden benötigt wird, nutzt diese Art des MDM-Systems die entsprechenden Quellsysteme, um einen Echtzeiteinblick zu gewähren. Allerdings ist eine zentrale Verwaltung der Daten – als Teil der Master Data Governance - notwendig, um sicherzustellen, dass der Golden Record in diesem Falle zuverlässig ist.

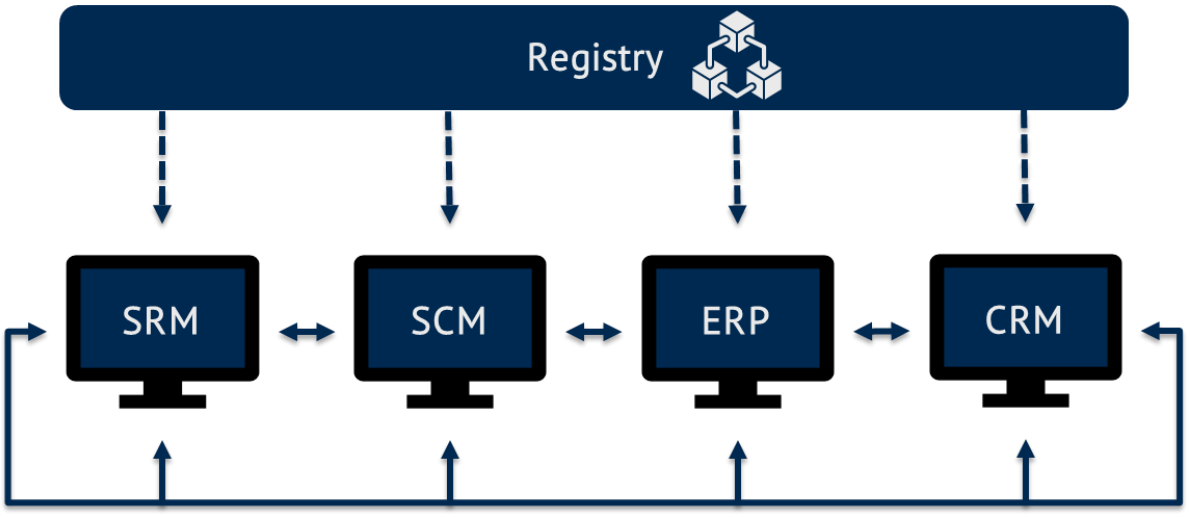

Abbildung 2: Registry Style (Beispiel)

Pros und Cons:

Da dieser Ansatz lediglich Referenzobjekte schafft, gestaltet sich die Implementierung weniger kosten- und zeitintensiv als bei dem Zentralisierungsansatz. Außerdem besteht ein sehr geringes Risiko bei der Implementierung, da das MDM-System lediglich einen Read-Only Zugang erhält und keine Änderungen an den Quellsystemen vorgenommen werden müssen. Nachteilig ist der Hohe Aufwand, der in das Metadatenmodell investiert werden muss, um die auf unterschiedliche Systeme verteilten Entitäten als Gesamtbild widerzuspiegeln. Darüber hinaus kann aufgrund der Verteilung der Daten das Reporting eine eingeschränkte Performanz aufweisen.

Zentralisierungs-/ Transaktionsansatz:

Bei der Zentralisierung werden die Stammdaten aus mehreren Quellsystemen inital zusammengetragen und in einen Hub importiert, der folglich als Single Source of Truth angesehen wird. So können die Daten für anschließende Analysen und Reporting genutzt werden. Im Fall einer Änderung an den Stammdaten wird der aktuelle Stand in die Quellsysteme zurückgespiegelt, sodass das MDM-System als Single Source of Truth gilt. Die Umsetzung geschieht häufig durch den Einsatz eines Enterprise Service Bus (ESB) und Service oriented Architecture (SOA).

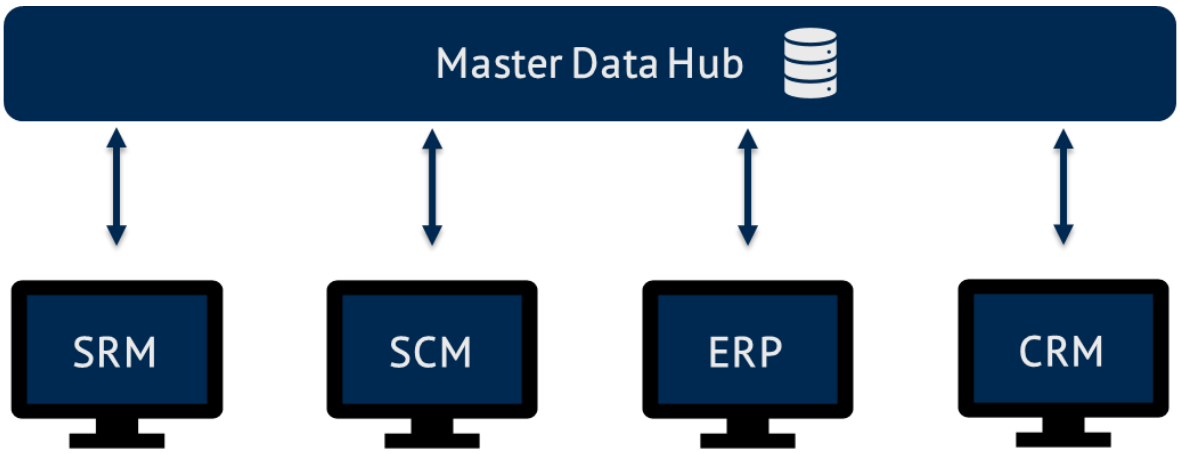

Abbildung 3: Zentralisierungs-/ Transaktions-Ansatz (Beispiel)

Pros und Cons:

Im Vergleich zu dem Registry-Ansatz kann die Implementierung der zentralisierten Lösung aufgrund der Modifikationen an den Peripheriesystemen kosten- und zeitintensiver ausfallen. Außerdem kann die Definition eines geeigneten Datenmodells zu einer Herausforderung werden, da es von allen Konsumenten akzeptiert werden muss. Die fortlaufende Wartung des MDM-Systems wird jedoch simplifiziert und die eindeutige Definition des MDM-Systems als Single Source of Truth vereinfacht sowohl Data Governance als auch Data Stewardship.

Hybrider Ansatz

Der Hybride MDM-Ansatz besteht aus einer Mischung beider zuvor beschrieben Ansätze. Sowohl die Anpassung der Daten im Rahmen des Zentralisierungsansatz als auch die Inperformanz des Reporting im Kontext des Register-Ansatzes werden ausgehebelt, indem der Hub neben den Identifikatoren auch entitäten-bezogene Attribute speichert. Das umfangreichere Datenmodell bietet eine gesteigerte Reporting-Geschwindigkeit. Im Gegensatz zum Zentralisierungsansatz verbleibt der Hub als System of Reference, da die Daten weiterhin in den Quellsystemen gepflegt werden.

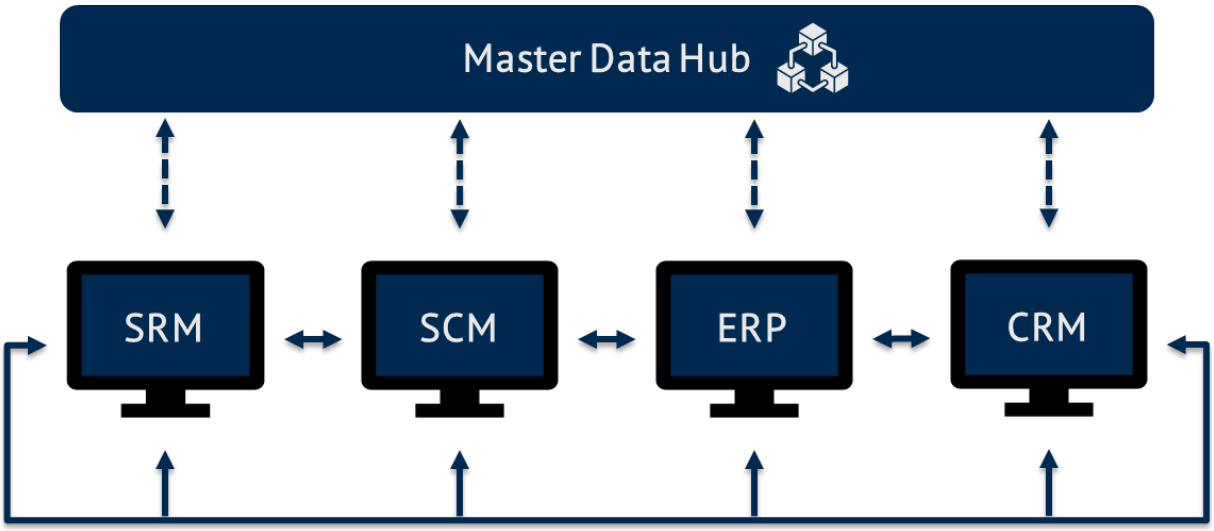

Abbildung 4: Hybrider Ansatz (Beispiel)

Pros und Cons:

Ein signifikanter Vorteil des hybriden Ansatzes ist die lose Kopplung zwischen Hub und Quellsystemen, sodass Migrationen oder Systemwechsel nur einen kleinen Konfigurationsaufwand Seitens des Hub in Anspruch nehmen. Ein möglicher Nachteil ergibt sich bei der Spiegelung der Attribute, wo ein Risiko für Inkonsistenzen besteht. Eine weitere Herausforderung ist, wie im Fall des Zentralisierungs-Ansatzes, die Definition des Datenmodells:

Während lediglich die Enterprise Master Data Attribute in den Hub aufgenommen werden müssen, verbleiben die Funktionsspezifischen Attribute für die Applikationen in den Quellsystemen. Außerdem muss definiert werden, welche Attribute als lokal und global gelten.

Folglich kann der hybride Ansatz aufgrund der losen Kopplung schneller implementiert werden, als der Zentralisierungs-Ansatz. Jedoch stellen die Definition des Datenmodells und die Harmonisierung des Update-Zyklus größere Herausforderungen dar, als im Fall des Registry-Ansatzes.

Exkurs: (Master) Data Governance

Abgeleitet von der Corporate Governance bestimmt (Master) Data Governance den Ordnungsrahmen bei der Umsetzung von Datenqualitätszielen. Hierfür werden Datenqualitätskriterien definiert, die die Zuverlässigkeit der Stammdaten garantieren sollen. Durch kontinuierliche Qualitätssicherung und Konsolidierung kann die Qualität bestehender Daten fortlaufend sichergestellt werden.

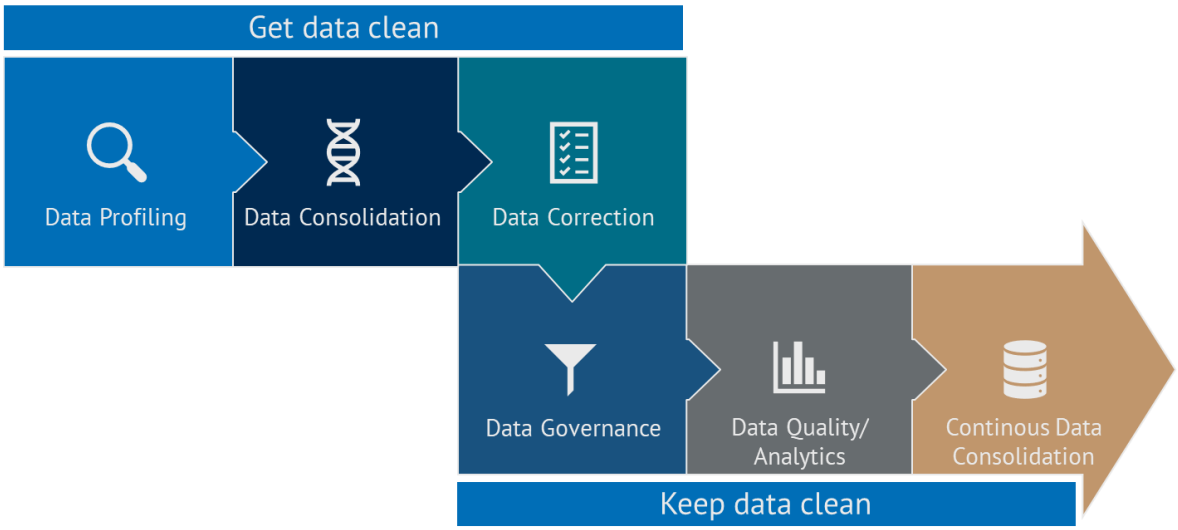

Abbildung 5: Master Data Management & Master Data Governance

Master Data Management als Enabler für Datenschutz-Compliance

Dr. jur. Kevin Marshall & Stephan Blazy

CEOs, Datenschutzbeauftragte IHK, Datenschutzauditoren TÜV (GDPC)

Master Data Management ist auch und gerade ein essenzieller Baustein einer adäquaten, transparenten und durchdachten DSGVO-Compliance im Unternehmen und besitzt daher auch zahlreiche datenschutzrechtliche Vorteile für Unternehmen und Behörden. Auch wenn die drei verschiedenen möglichen Methoden der Implementierung eines MDM teilweise unterschiedliche Rechtsprobleme aufwerfen, so ist allen Ansätzen gemein, dass sie übergeordnet einen wesentlichen Beitrag zur DSGVO-Compliance leisten können, der nachfolgend skizziert wird.

Durch ein MDM können u.a. die Betroffenenrechte, die Datenschutz-Grundsätze sowie zahlreiche weitere DSGVO-Pflichten, wie beispielsweise Privacy by Design und by Default (Art. 25 DSGVO), besser umgesetzt werden. So stellen etwa isolierte Datensilos innerhalb von Unternehmen ein Compliance-Risiko für die datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Datensparsamkeit-/Minimierung und der Speicherbegrenzung dar, denen zu begegnen.

Durch ein MDM, mit einem zentralisierten SSOT, kann auch dem Recht auf transparente und vollständige Datenlöschung (Art. 17 DSGVO) effektiver nachgekommen werden. Vergleichbares gilt auch allgemein für die Transparenz der Datenverarbeitung (Art. 5, Art. 12 DSGVO), bei der u.a. Datenquellen, Datenarten, Datenflüsse und Datenzugriffe im Vordergrund stehen und die der Verantwortliche nachweisen können muss (s. Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

Förderung von Zugriffs- und Berechtigungskonzepten

So muss der Zugriff auf durch MDM strukturierte Daten streng an dem datenschutzrechtlichen Grundsatz der Erforderlichkeit ausgerichtet werden, so etwa, wenn nur die tatsächlich zuständigen Abteilungen und Entscheidungsträger auf bestimmte und für deren Aufgabe erforderliche Daten am SSOT zugreifen können. Auch können die einzelnen Business Objects für verschiedene Abteilungen verkürzt auf die relevanten Informationen ausgegeben werden, wodurch ebenso ein rechtlich gefordertes Zugriffs- und Berechtigungskonzept, das gerade in großen international agierenden Unternehmen oft eine große Herausforderung darstellt, überhaupt erst adäquat technisch und organisatorisch verwirklicht werden kann. Insbesondere im Hinblick auf den Zentralisierungs-/Transaktionsansatz ist es von besonderer Bedeutung, dass verschiedene Rechte und Zugriffe so implementiert werden, dass Zugriffe auf die entsprechenden Quellsysteme nur durch die zuvor definierten Berechtigten erfolgen kann.

Ein datenschutzrechtlich erforderlicher Zugriffs- und Freigabeprozess zur Stammdatenänderung wird aktuell noch eher stiefmütterlich behandelt. Eine solcher Prozess, der mit entsprechenden Maßnahmen zu hinterlegen ist, ist aber wesentlich für die Gewährleistung des Grundsatzes der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO). Datenaktualität, sachliche Datenwahrheit und Datenvollständigkeit (Datenqualitätsziele) sind die zu gewährleistenden Kernelemente dieses Grundsatzes, deren Umsetzung etwa durch den automatisierten Abgleich von Referenzobjekten mit den Quellsystemen unterstützt werden kann. Durch die Gewährleistung von Datenrichtigkeit, können auch zivilrechtliche Streitigkeiten und operative und prozessrechtliche Kosten reduziert bzw. vermieden werden. Unter Bezugnahme auf das Eingangsbeispiel der Warenbestellung und der Bedeutung einer korrekt hinterlegten Adresse und korrekten Zahlungsdaten, kann das Risiko von verspäteten Lieferungen oder unberechtigten Mahnungen deutlich verringert werden.

MDM unterstützt Nachweispflichten des Unternehmens

Eine entsprechende Prozessbeschreibung und Protokollierung der einzelnen Schritte, etwa der Protokollierung von Zugriffen und Änderungen an den Stammdaten, ist zudem wesentlich zur Gewährleistung der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) und der Datensicherheit (Art. 32 DSGVO), da Handlungen und Aktionen innerhalb von komplexen und grundsätzlich intransparenten Systemen nur schwer nachvollziehbar und damit schädlich für die DSGVO-Compliance sind. Das Fundament datenschutzrechtlicher Transparenz kann hier bspw. eine IT-Landscape-Analyse schaffen, welche dem Datenschutzbeauftragten zugleich auch die Ausübung seiner Aufgaben erleichtert.

Datenschutzrechtliche Risiken durch MDM begleiten und covern

Jedoch müssen gleichzeitig auch die durch ein MDM hervorrufbaren Risiken für die DSGVO-Compliance reduziert werden. Ein MDM sollte daher nicht ohne datenschutzrechtliche Begleitung implementiert werden, da hierbei einige Rechtsfragen zu klären sind, wie etwa der geografische Speicherort der Daten am SSOT, die Zugriffsberechtigungen sowie die (auch datengeprägte Definition) von Datenqualitätszielen und die diese Ziele umsetzenden Datenqualitätskriterien.

So muss sich das MDM insbesondere an den Richtlinien des unternehmensinternen Datenschutzmanagementsystem orientieren, um Inkonsistenzen zu vermeiden. Ähnliches gilt für die mit der Zentralisierung der Daten einhergehenden Profiling-Möglichkeiten, etwa durch event-logs, sowie der mit einer Zentralisierung von Daten einhergehenden größeren IT-Gefährdung, deren unter Berücksichtigung von Maßnahmen zur Datensicherheit (Art. 32 DSGVO) begegnet werden muss. So sind etwa auch die Definierung der Update-Zyklen zwischen den Quellsystemen und des SSOT von Bedeutung. Je engmaschiger diese definiert sind und ggf. in Echtzeit vollzogen werden, desto eher kann dem Grundsatz der Datenrichtigkeit entsprochen werden.

Ebenso sollte im Rahmen eines **MDG** definiert und hinterlegt werden, welche Datenattribute und ggf. welche Quellsysteme als Referenz für etwaige Datenanalysen in rechtlich zulässiger Weise verwendet werden (dürfen), insbesondere, wenn es sich bei den Daten um personenbezogene oder beziehbare Daten handelt, wie etwa die Handelsumsätze eines Einzelunternehmens.

Auswirkungen des Brexit auf MDM und DSGVO-Compliance

Auch der Brexit besitzt rechtliche Implikationen, denen die Modellierung und Integration eines MDM folgen muss. Der Brexit, insbesondere ein no-deal-Szenario, wird zahlreiche Auswirkungen auf die DSGVO-Compliance von Firmen haben, die mit britischen Unternehmen zusammenarbeiten, Daten übermitteln, ihren Hauptsitz dort haben oder ihr Stammdatenmanagement auf Server in UK vorhalten. So wird UK, unabhängig der DSGVO-Compliance der dortigen Unternehmen, als sog. Drittland angesehen. Für eine Datenübermittlung oder einen Datenaustausch in Drittländer (UK) ist eine gesonderte Rechtsgrundlage erforderlich, sodass künftig hier insgesamt höhere rechtliche Voraussetzungen existieren. Sofern eine baldige Angemessenheitsentscheidung der EU-Kommission zum Datenschutzniveau in UK nicht vorliegt (eine solche wird in Fachkreisen auch nicht zeitnah erwartet), bleiben nur die Möglichkeiten des Abschlusses von Standardvertragsklauseln mit in UK ansässigen Partnern oder – für die Datenverarbeitung innerhalb eines Konzerns – die Ausarbeitung sog. Binding Corporate Rules, die Zeit kosten und aufsichtsbehördlich genehmigt werden müssen. Gerade dieser Aspekt ist auch für ein unternehmensweites MDM von großer Bedeutung, z.B. für die Bestimmung des SSOT im Rahmen der Informationsobjektarchitektur. Denn mit der Veränderung/Verlagerung des Speicherorts der (Stamm-)Daten, womit es sich um eine rechtfertigungsbedürftige Datenverarbeitung handelt, gehen zahlreiche rechtliche Fragen einher, die zuvor – etwa durch den Datenschutzbeauftragten – zu klären sind.

Insofern muss ein MDM auf die rechtlichen Gegebenheiten und Veränderungen adäquat reagieren, z.B. durch die vorherige Identifizierung ob und welche personenbezogenen Stammdaten in UK transferiert werden dürfen und durch technische und organisatorische Beschränkungen des Datenzugriffs-/Abrufs innerhalb mehrerer Entitäten.

Fazit

Ein MDM sollte nicht ohne datenschutzrechtliche „Brille“ auf die Umstrukturierung eingeführt werden, die dabei entstehenden Compliance-Risiken würden die Chancen nämlich wieder kompensieren und es wäre nichts gewonnen. Ein gut durchdachtes MDM-Projekt berücksichtigt daher stets auch datenschutzrechtliche Aspekte bei der Planung, Ausgestaltung und Einführung und beleuchtet hierbei beide Seiten der MDM-Medaille aus technischer und rechtlicher Sicht.