So sollten Unternehmen ihre Daten kategorisieren

Teil 1 der Beitragsserie „Profitipps zum Data Compliance Management“

Im Rahmen ihrer digitalen Transformation einer regulatorischen und rechtlichen Komplexität ausgesetzt. Das unterstreicht die Notwendigkeit eines präzisen Verständnisses und eines robusten Managements der eigenen Daten. Diese dreiteilige Serie beschreibt die aus Sicht von Praktiker:innen relevantesten Aspekte und bewährte Herangehensweisen.

Im Zentrum dieses ersten Beitrages steht die Kategorisierung der Unternehmensdaten. Das ist eine Grundvoraussetzung für einen rechtskonformen Umgang mit Daten. In der Praxis werden die regulatorischen Aspekte jedoch oft zu wenig berücksichtigt.

Die praktische Bedeutung der Datentransparenz

Fundamental ist zunächst, dass das Unternehmen weiß, welche Daten es überhaupt hält. Außerdem ist wichtig, dass es Kenntnis darüber hat, wie die Daten verarbeitet werden und in welchem Kontext dies geschieht. Nur so kann das Unternehmen beurteilen, welche rechtlichen Aspekte für bestimmte Daten überhaupt relevant sind. Datenschutzrecht, Urheberrecht oder Geheimnisschutzrecht können sehr konkrete Anforderungen an den Umgang mit Daten stellen. Und um diese zu erfüllen, benötigt das Unternehmen ein gesundes Maß an Datentransparenz.

Der Kontext als Schlüssel zu einem rechtskonformen Umgang mit Daten

Dazu gehört aber nicht nur die Kenntnis, welche Daten es überhaupt gibt. Noch wichtiger ist die Information, in welchem Kontext sie zu betrachten sind. Erst der Kontext gibt Aufschluss über den Ursprung der Daten, ihre Eigenschaften, ihre prozessuale Bedeutung und damit über die zugehörigen Compliance-Anforderungen. Beispielsweise reicht die Information, dass bestimmte Daten bei der HR-Abteilung verarbeitet werden und irgendwo in der HR-Software gespeichert sind, nicht aus, um die damit möglicherweise ausgelösten regulatorischen Pflichten zu verstehen. Wenn Daten etwa personenbezogen sind und direkt von Betroffenen stammen, müssen diese darüber formal informiert werden. Wenn Daten geheimnisschutzrelevant sind, müssen sie unter Umständen besonders markiert und geschützt werden. Und wenn sie urheberrechtlich geschützt sein könnten, käme es darauf an, ob das Unternehmen selbst der Träger der entsprechenden Rechte ist oder vielleicht jemand anderes.

Folgen einer ungenauen Kategorisierung

In der Praxis werden immer noch viel zu häufig Datenkategorien auf Grundlage der verwendeten IT-Systeme oder nach Maßgabe der innerbetrieblichen Zuständigkeiten definiert. Eine solche, nicht-kontextbezogene Datenkategorisierung ist jedoch nicht nur ungenau, sondern kann auch drastische praktische Konsequenzen haben. Ein Beispiel: Werden Gesundheitsdaten (wie Schwerbehinderungsgrade) versehentlich einer anderen Datenkategorie zugeordnet, etwa „Bewerberdaten“, hätte das nach der neueren EuGH-Rechtsprechung unter

Umständen zur Folge, dass der gesamte Datenbestand „Bewerberdaten“ den erheblich höheren Schutzvorgaben für Gesundheitsdaten unterliegen würde. Wenn das Unternehmen dies nicht weiß und es folglich operationell nicht berücksichtigt, drohen empfindliche Bußgelder und Reputationsschäden.

Mehrdimensionale Datenkategorisierung

Datenkategorien sollten daher immer kontextbezogen entwickelt werden. Ideal eignen sich hierfür standardisierte hierarchische Geschäftsprozessmodelle, wie sie von bestimmten Organisationen zur Verfügung gestellt werden. Von den dort umfassend definierten Prozessgruppen und den in ihnen zusammengefassten Prozessen lassen sich prozessbasierte Datenkategorien ableiten und an die spezifischen Besonderheiten des Unternehmens anpassen. Diese können dann mit den notwendigen Attributen versehen werden, wie „personenbezogen“, „besondere Kategorie i.S.v. Art. 9 DSGVO“ oder „geheimnisschutzrelevant“.

Erfassung aller Unternehmensdaten

Ein Vorteil dieser Herangehensweise ist, dass sie alle Unternehmensdaten erfasst und damit eine effektive Datenkategorisierung ermöglicht. Eine selektive Betrachtung hingegen birgt Risiken. Schon durch eine Verknüpfung von davor datenschutzrechtlich unbedenklichen Daten kann beispielsweise plötzlich Personenbezogenheit im Sinne der DSGVO entstehen. Die Folge: Ab dem Moment gelten völlig neue Anforderungen für die zukünftige rechtskonforme Handhabung dieser Daten. Das wird bei einer selektiven und dadurch notgedrungen fragmentierten Kategorisierung der Datenbestände leicht übersehen.

Fazit

Eine gründliche Datenkategorisierung, ausgerichtet an regulatorischen Anforderungen und dem Kontext der zugrundeliegenden Geschäftsprozesse, ist das Fundament eines resilienten Daten-Compliance-Managements. Durch eine solide Datenkategorisierung können Unternehmen ihre Compliance-Risiken minimieren und eine klare Linie im Umgang mit unterschiedlichen Datentypen zeichnen. In den nächsten beiden Beiträgen werden wir ein Verständnis für den Data Lifecycle schaffen und uns dann der Frage widmen, wie ein Unternehmen auf Grundlage seiner ordentlich kategorisierten Datenbestände in effektiver und effizienter Weise Daten-Compliance sicherstellen kann.

Ansprechpartner:

Dr. Jyn Schultze-Melling, LL.M.
Tel: +49 30 530199 410
jschultzemelling@kpmg-law.com