Der Lebenszyklus von Daten und seine Bedeutung aus rechtlicher Sicht

Teil 2 der Beitragsserie „Profitipps zum Data Compliance Management“

Nachdem im ersten Teil der Beitragsserie die Grundlagen der Datenkategorisierung beschrieben wurden, betrachten wir nun den gesamten Lebenszyklus der Daten von Unternehmen. Die Compliance-Anforderungen variieren nämlich je nachdem, ob es gerade um die Datenerhebung, -verarbeitung, -speicherung oder -löschung geht. Ein durchdachtes Vorgehen ist daher essenziell, um regulatorische Fallstricke zu vermeiden.

Phase 1 des Lebenszyklus von Daten: Datenerhebung

Unternehmen erheben Daten aus den verschiedensten Gründen, sei es zur Kundenkommunikation, zur Produktentwicklung, zur Verwaltung, zur Vertragsabwicklung oder zur Erfüllung gesetzlicher Pflichten. Die Zweckbestimmung spielt aus regulatorischer Sicht eine fundamentale Rolle.

Wenn es sich um bereits vorhandene Daten handelt, die ursprünglich zu einem anderen Zweck generiert worden sind, kann es sein, dass schon dieser Umstand die geplante Neuerhebung der Daten vereitelt oder zumindest deutlich erschwert.

Manche Daten dürfen aber unter Umständen grundsätzlich schon gar nicht erst erhoben werden, etwa wenn dies einen Verstoß gegen gesetzliche oder vertragliche Verpflichtungen des Unternehmens bedeuten würde. In der Praxis betrifft das zum Beispiel häufig Dienstleister, die Daten im Auftrag ihrer Kunden verarbeiten. Was nicht alle wissen: Aufgrund der Regelungen der DSGVO dürfen diese Daten noch nicht einmal zur Erhöhung des Sicherheitsniveaus, und erst recht nicht zur Verbesserung der eigenen Prozesse oder Produkte verwendet werden.

Manche Daten sind urheberrechtlich geschützt und dürfen nur mit der ausdrücklichen Erlaubnis des Rechteinhabers erhoben und verwertet werden Und: Nicht nur Gesetze, sondern auch vertragliche Verpflichtungen können die Datenerhebung verbieten. Vertraulichkeitsvereinbarungen, Kooperationsverträge und Lizenzbestimmungen sind weitere potenzielle Stolpersteine.

Aber selbst bei der Neugenerierung von Daten sind gesetzliche und regulatorische Aspekte zu berücksichtigen. So können Einwilligungen von Betroffenen, behördliche Genehmigungen und andere Voraussetzungen erforderlich sein. Die Herkunft von Daten spielt eine wesentliche Rolle, da sie den rechtlichen Rahmen mitdefiniert. Sie sollte daher unbedingt dokumentiert werden, um die Einhaltung regulatorischer Vorgaben zu belegen und die Rechtmäßigkeit der Datennutzung zu gewährleisten.

Phase 2 des Lebenszyklus von Daten: Datenverarbeitung

Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden. Das ergibt sich aus den

Prinzipien der Datenminimierung der der Zweckbindung der DSGVO. Das gilt ganz besonders für die Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO, wie etwa Gesundheitsdaten, da hier höhere Schutzstandards gelten. Auch die Weitergabe von Daten an Dritte oder die Verarbeitung für neue, ursprünglich nicht vorgesehene Zwecke, kann regulatorische Implikationen haben. In diesen Fällen ist eine sorgfältige Prüfung der Rechtsgrundlagen und gegebenenfalls eine erneute Zustimmung der Betroffenen erforderlich. Und das hat sehr praktische Auswirkungen. Eine vor Jahren erteilte Einwilligung kann ihre legitimierende Wirkung schlicht durch Zeitablauf verlieren, was unter Umständen eine ganze Marketing-Kampagne zu einem Haftungsfall werden lassen kann. Typischerweise sind es aber gesetzliche Änderungen oder geänderte behördliche Ansichten, die dazu führen, dass Unternehmen eine langjährige Praxis der Datenverarbeitung überprüfen sollten.

Phase 3 des Lebenszyklus von Daten: Datenspeicherung

In der dritten Lebenszyklusphase, der Datenspeicherung, stellt sich vor allem die Frage, wie lange Daten gespeichert werden dürfen. Hier kollidieren die gesetzlichen Anforderungen: Während das Datenschutzrecht eine Löschung verlangt, sobald Daten nicht mehr für ihren ursprünglichen Zweck gebraucht werden, verlangen unter anderem handels- und steuerrechtliche Regelungen eine längerfristige Archivierung. Unternehmen sollten daher die Aufbewahrungsfristen klar und spezifisch für jede betroffene Jurisdiktion definieren und für jede Datenkategorie individuell festlegen. Hierbei ist eine transparente und effiziente Datenarchitektur entscheidend, um den Überblick zu behalten und Compliance-Anforderungen auch über nationale Grenzen hinweg verlässlich zu erfüllen.

Auch sollten Unternehmen klären, wo die Daten gespeichert werden. Denn jede Übermittlung von Daten erfordert nach den Regelungen der DSGVO eine Rechtsgrundlage – sei es zu einem lokalen Rechenzentrum oder direkt in die Cloud. Wenn grenzüberschreitend gearbeitet wird – was gerade bei multinationalen Konzernen keine Seltenheit ist – sind weitere gesetzliche Anforderungen zu beachten. Zum Beispiel wären dann gegebenenfalls weitere Verträge abzuschließen. Auch die Dokumentation kann dann aufwändiger sein.

Phase 4 des Lebenszyklus von Daten: Datenlöschung

Am Ende des Lebenszyklus der Daten steht die systematische Löschung. Gründe für die Löschung sind der Ablauf der Aufbewahrungsfristen und Anfragen der Betroffenen. Automatisierte Löschprozesse können dabei helfen, die Einhaltung der Löschfristen sicherzustellen und das Risiko von Datenschutzverletzungen zu minimieren. Hierfür ist es essenziell, die Löschprozesse sorgfältig zu dokumentieren, um das Einhalten der gesetzlichen Regelungen belegen zu können. Wenn dritte Dienstleister mit der Löschung oder Vernichtung von Daten beauftragt werden, müssen ebenfalls robuste vertragliche Grundlagen geschaffen werden, um die Vertraulichkeit der Daten auch auf ihrem letzten Weg sicherzustellen.

Fazit

Wenn Unternehmen ihre Daten im Vorfeld sauber kategorisieren, können sie sie in den verschiedenen Lebenszyklen differenziert betrachten und handhaben. Dies bietet einen umfassenden Rahmen für das Daten-Compliance-Management. Durch eine tiefergehende Auseinandersetzung mit den Anforderungen jeder einzelnen Phase und dem Implementieren von entsprechenden Prozessen können Unternehmen ihre Maßnahmen zur Sicherstellung der Rechtskonformität optimieren und regulatorische Risiken minimieren.

Der dritte und letzte Teil dieser Beitragsserie befasst sich mit dem Data Compliance Management und den damit verbundenen praktischen Herausforderungen für Unternehmen.

Ansprechpartner:

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