# Daten-verantwortung wahrnehmen

Die neue Datenschutzverordnung der EU stellt auch den CIOs in der Schweiz eine weitere komplexe Aufgabe. Wie beginnen? Mit den richtigen Fragen gelangen Sie in kurzer Zeit zu einer fundierten Standortbestimmung.

→ VON DANIEL SEILER

## DER AUTOR

**Daniel Seiler,**
lic. iur., ist Manager im Information Governance & Compliance Team bei KPMG Schweiz. Er ist spezialisiert auf die Schnittstelle zwischen Recht, IT und Business und verfügt über langjährige Erfahrung beim Umgang mit rechtlichen Fragestellungen im IT-Umfeld (z.B. Cloud, Outsourcing, digitale Transformation und Datenschutz).
→ www.kpmg.ch

Ein internationales Unternehmen mit Sitz in Europa hat sich aus Kostengründen dazu entschieden, sein bisheriges Datacenter durch eines im nahen Ausland zu ersetzen. Das Projekt steht, das neue Datacenter wird aufgebaut und die Systeme werden integriert. Kurz vor dem geplanten Datentransfer stellt sich jedoch heraus, dass einzelne Datensätze spezifischen Regulationen unterliegen, die den Transfer ins Ausland verbieten. Nun kann einerseits das neue Datacenter nicht vollständig in Betrieb genommen werden, andererseits muss das bestehende weiterlaufen. Das Unternehmen muss somit die Betriebskosten beider Center für eine längere Zeit finanzieren. Hätte das Unternehmen frühzeitig abgeklärt, über welche Art von Daten es verfügt und wie diese zu handhaben sind, hätte es viel Zeit und Geld gespart.

### Datenschutz ist Sache der Geschäftsleitung

Das obige Beispiel ist zwar erfunden, aber keineswegs aus der Luft gegriffen. Mit der neuen Datenschutz-Grundverordnung (DSGVO) hat das Europaparlament die umfangreichste Revision im Bereich des Datenschutzes der letzten Jahrzehnte verabschiedet. Sie tritt im Mai 2018 in Kraft und enthält zahlreiche neue Bestimmungen, die sich geschäftskritisch auswirken können. Sie erfordern, je nach Unternehmensstruktur, tiefgreifende Veränderungen organisatorischer und technischer Art.

Wie in der letzten Computerworld ausgeführt, sind davon auch Schweizer Firmen betroffen (vgl. «Datenschutz: Was uns das EU-Recht angeht», Computerworld 6/2016, ab S. 62). Die DSVGO ist anwendbar auf «alle Unternehmen und Organisationen, die in der EU ansässigen Personen Güter oder Dienstleistungen anbieten» sowie auf «Unternehmen und Organisationen, die das (Online-)Verhalten von diesen Personen überwachen». Das bedeutet, dass ein Schweizer Unternehmen unter die DSGVO fallen kann, auch wenn es keine Niederlassung in der EU hat. Zum Beispiel, wenn:

- das Unternehmen Datenverarbeitungen in einem EU Staat vornimmt, z.B. im Rahmen eine IT-Outsourcings oder eines Datacenters im EU-Ausland;
- die Firma in ihrem Online-Shop Produkte auch an Personen in der EU anbietet;
- ein Subunternehmer des Schweizer Unternehmens Personendaten der Angestellten aus der EU verarbeitet;
- die Schweizer Firma Daten über das (Online-) Verhalten von Produktnutzern für Marketingzwecke sammelt.

Selbst wenn eine Schweizer Firma nicht direkt betroffen ist, gilt es die aktuellen Entwicklungen zu beachten, denn es ist davon auszugehen, dass sich das schweizerische Datenschutzrecht wie schon bis anhin stark an der EU-Regulierung anlehnt. Andernfalls würden die Geschäfte von Schweizer Unternehmen mit der EU erheblich erschwert.

Die jetzt anstehenden Aufgaben müssen der Geschäftsleitung bekannt sein und auch auf dieser Stufe angegangen werden. Unter keinen Umständen sollte das Thema Datenverantwortung allein in die IT oder die Linie delegiert werden, da dort meist kein Gesamtüberblick über das Unternehmen vorhanden ist. Nachfolgend einige Punkte, welche die Bedeutung des Themas für die Geschäftsleitung verdeutlichen.

### Hohe Bussen bei Nichteinhaltung

Bei Verstoss gegen die DSVGO-Bestimmungen können von den entsprechenden lokalen Datenschutzbehörden Bussen in der Höhe von bis zu 20 Mio. EUR oder höchstens 4 Prozent des Jahresumsatzes verhängt werden. Die Bussen sind grundsätzlich vom Unternehmen zu tragen. Sollte aber die verantwortliche Person im Unternehmen z. B. wegen Unterlassungen (z. B. wenn Prozesse nicht überprüft wurden) zu dem Verstoss gegen die DSGVO beigetragen haben, kann unter Umständen Regress auf diese Person genommen werden, was dann eine persönliche Haftung bedeuten würde. Verglichen mit den heutigen Verhältnissen ist das eine radikale Verschärfung. Zwar können zur Schadensbegrenzung Versicherungslösungen ins Auge gefasst werden, sowohl für das Unternehmen wie auch die Mitglieder der Geschäftsleitung. Dies setzt aber voraus, dass die entsprechenden Bedingungen des Versicherers erfüllt sind (z.B. Anforderungen an die Governance und Überprüfungsprozesse).

### Meldepflicht für Datenschutzverletzungen

Die DSGVO verpflichtet Unternehmen dazu, Datenschutzverletzungen der lokalen Datenschutzbehörde zu melden. Die Meldung muss spätestens 72 Stunden nach Entdecken des Vorfalls erfolgen, beziehungsweise sofort, wenn eine grobe Verletzung der Privatsphäre vorliegt.

Datenschutzverletzungen geschehen manchmal unabsichtlich: Etwa, wenn ein Mitarbeiter Dokumente im Zugabteil liegen lässt, Personendaten auf Social-Media-Kanälen postet oder an den falschen Empfänger sendet. Der Datenschutz wird aber auch verletzt, wenn für das Verarbeiten der Daten kein ausreichender Grund besteht (z.B. im Fall von Personendaten, die für den ursprünglichen Zweck nicht notwendig wären), oder wenn die Personendaten nicht adäquat geschützt werden (z.B. durch Verschlüsselung). Technische Vorkehrungen wie die Anonymisierung oder Tokenisierung von Daten können Datenschutzverletzungen minimieren. Jedoch gilt es, die Technologien sinnvoll in die eigene Systemlandschaft zu integrieren, um sicherzustellen, dass alle kritischen Vorgänge adäquat abgesichert sind.

Nur zu wissen, dass eine Meldepflicht existiert, genügt daher nicht. Schon um Datenschutzverletzungen überhaupt zu erkennen und zu bewerten, sind technische Massnahmen nötig – erst recht, um sie zu verhindern oder um innert der vorgeschriebenen 72 Stunden zu reagieren.

### Obligatorischer Datenschutzbeauftragter

Die DSGVO macht in vielen Fällen die Ernennung eines Datenschutzbeauftragten im Unternehmen obligatorisch. Dies ist etwa der Fall, wenn pro Jahr die Daten von mehr als 5000 Personen bearbeitet werden. Der Datenschutzbeauftragte muss über Fachwissen bezüglich Datenschutzgesetzgebung und -praxis verfügen sowie seine Rolle genügend unabhängig ausüben können. Unter Umständen sind auch bei Fachpersonen Zusatzausbildungen nötig. Ausserdem ist die organisatorische Eingliederung ins Unternehmen zu klären. Es dürfte daher sinnvoll sein, sich bereits jetzt damit zu beschäftigen, wie dies umgesetzt werden soll. Schon heute können Fachausbildungen geplant oder organisatorische Veränderungen entworfen werden.

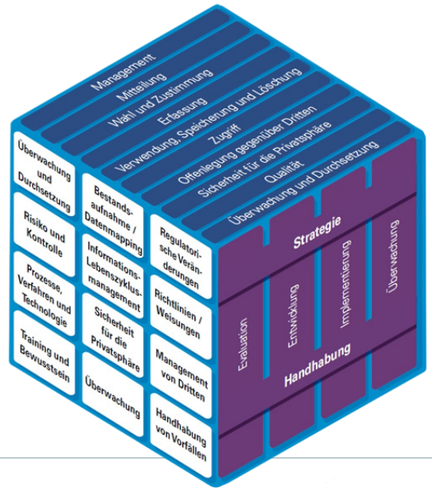
Die Rolle des Datenschutzbeauftragten darf auch von einem externen Dienstleistungsunternehmen ausgeübt werden. Je nach Unternehmensgrösse ist das die kostengünstigere Lösung. Selbstverständlich muss auch in diesem Fall darauf geachtet werden, dass der Dienstleister über das notwendige Datenschutz-Fachwissen verfügt. Unabhängig von der gewählten Lösung muss der Datenschutzverantwortliche inkl. Kontaktdaten an die zuständige Datenschutzbehörde gemeldet werden.

### Weitere kritische Neuerungen

**Folgenabschätzung:** Falls die Datenverarbeitung hohe Risiken für die Privatsphäre zur Folge haben könnte, verpflichtet die DSGVO Unternehmen zu einer Datenschutz-Folgenabschätzung. Resultiert daraus tatsächlich ein hohes Risiko, muss vor Beginn der Verarbeitung die zuständige Datenschutzbehörde konsultiert werden. Dies kann weitreichende Folgen für die Inbetriebnahme von neuen Datenverarbeitungssystemen haben. Es ist eine sorgfältige Überprüfung durchzuführen um zuverlässig zu eruieren, welches Risiko die geplanten Verarbeitungsvorgänge bzw. Systeme allenfalls aufweisen. Die DSGVO verpflichtet daher Unternehmen zu einem entsprechenden Risikomanagement.

**Daten Lifecycle Management:** Durch die DSGVO können Personen von Unternehmen verlangen, dass Daten über sie gelöscht werden. Dabei liegt es in der Verantwortung des Unternehmens, die Daten vollständig und korrekt zu löschen (in der Regel liegt diese Verantwortung beim Dateneigner im Unternehmen bzw. bei der IT für die Umsetzung). Dies setzt voraus, dass die gesamte Datenlandschaft und die unterschiedlichen Daten-Pool überhaupt durchsucht werden können. Was oft vergessen wird: Hier gehören auch die Daten dazu, welche allenfalls bei einer Drittpartei aufbewahrt werden. Um diesen Anforderungen gerecht zu werden, ist es unbedingt notwendig, eine Data-Governance sowie ein Daten Lifecycle Management zu implementieren, welche sehr hohen Standards genügt.

### Rahmenwerk zum Datenschutz




Die wichtigsten Themen, Prozesse und Projektphasen für einen strukturierten, gesetzeskonformen Datenschutz

Quelle: KPMG

### Standortbestimmung

Der CIO trägt Verantwortung für den Schutz derjenigen Daten, welche IT-basiert verarbeitet werden. Dies schliesst auch Daten ein, die durch Dritte (z.B. bei einem Outsourcing) verarbeitet werden. Damit hat der CIO ein weites Feld von Themen, Prozessen, Systemen, Anspruchsgruppen und Technologien zu koordinieren. Um dieser Verantwortung gerecht zu werden, sollte der CIO ein Vorgehen wählen, das gezielt die wichtigen und risikobehafteten Themen angeht und Lücken schnell sichtbar macht. Die Fragen in der Checkliste (S. 20) sollen eine Hilfestellung für den CIO sein, um eine erste Bestandsaufnahme im Unternehmen durchzuführen. Zwar muss der CIO nicht alle Fragen selber beantworten können. Lassen sich die Fragen aber auch durch die zuständigen Fachkräfte in der IT, der Rechtsabteilung etc. nicht genügend konkret beantworten, so kann dies ein Hinweis auf Defizite in diesem Bereich sein, weshalb sich dort eine vertiefte Überprüfung empfiehlt. Eine solche Überprüfung sollte in einen Bericht an den CIO münden, damit darauf basierend die entsprechenden Risiken ausgewiesen und die Behebung von allfälligen Defizite vorgenommen bzw. geplant werden können. →

# «Datenschutz ist heute Chefsache und darf auf keinen Fall nur der IT überlassen werden»

Daniel Seiler

**Analyse, Umsetzung, Überprüfung**

Die Zeitspanne bis 2018 mag auf den ersten Blick komfortabel erscheinen. Allerdings kommen nicht nur technische Anpassungen auf den CIO zu. Auch die Unternehmensleitung als Ganzes muss Prozesse neu aufbauen, Verantwortungen für den Datenschutz regeln, Datenschutzverantwortliche einsetzen und das Risiko-Management anpassen. Wie geht man dabei vor?

Zuerst sollte genau analysiert werden, von welchen Regelungen die Daten des Unternehmens betroffen sind. Dabei ist nicht nur die DSGVO zu beachten, sondern je nach Tätigkeitsfeld auch Bankenrecht, Gesundheitsrecht, Güterkontrolle oder Exportkontrolle. Daher braucht es zunächst eine Bestandesaufnahme über die Art der vorhandenen Daten. Sind die Daten erst einmal kategorisiert, ist es bedeutend einfacher, abzuklären, welcher Regulation die verschiedenen Datenkategorien unterliegen. Anschliessend sind die Anforderungen aus der einschlägigen Regulation strukturiert aufzunehmen (z.B. mittels einer Anforderungsliste) und konkrete technische oder organisatorische Massnahmen daraus abzuleiten. Dies kann beispielsweise bedeuten, dass Daten verschlüsselt werden müssen oder in einem bestimmten Land aufzubewahren sind, oder aber dass der Zugang zu den Daten definierten Personenkreisen vorbehalten bleibt.

Aufgrund dieser Analyse lässt sich eine Strategie entwickeln, die einen Projektplan sowie eine Roadmap umfasst. Diese zeigt auf, welche Massnahmen getroffen werden müssen, um den regulatorischen Anforderungen zu entsprechen. Anschliessend müssen die Massnahmen sehr strukturiert umgesetzt werden. Insbesondere ist auf die Zeitplanung und die Verantwortlichkeiten zu achten. Nach der Umsetzung ist die Arbeit jedoch noch nicht getan. Es ist wichtig, regelmässig zu überprüfen, wie sich die Massnahmen auswirken, ob Anpassungen der Massnahmen notwendig sind und ebenfalls, ob aufgrund veränderter Rahmenbedingungen ein Eingreifen erforderlich ist (z.B. wegen Gesetzesänderungen, Technologieveränderungen etc.). Schliesslich kann die Unternehmensleitung in Erwägung ziehen, die Leistungen z.B. im Bereich Datenschutz zertifizieren zu lassen, um so den internen Anspruchsgruppen wie auch den Kunden zu bestätigen, dass die Datenverantwortung im Unternehmen einen hohen Stellenwert geniesst und diese professionell und strukturiert umgesetzt wird. ←

## Checkliste: 20 Fragen für den CIO

1 Ist in meinem Unternehmen bekannt, welche (Personen-)Daten verarbeitet werden, wo sich diese befinden und wer sie verwaltet?

2 Verarbeitet das Unternehmen besonders schützenswerte Personendaten wie ethnische Zugehörigkeit, politische Einstellung oder Gesundheit?

3 Werden Daten verarbeitet, die einer Geheimnispflicht unterliegen, wie Bankkunden-, Arzt-, Anwalts- oder Amtsgeheimnis?

4 Werden Daten grenzüberschreitend übertragen (z.B. in die EU oder USA)?

5 Nutzt das Unternehmen eine Form von Cloud Computing?

6 Werden Unternehmensprozesse durch Dritte durchgeführt und/oder wurde die IT ausgelagert?

7 Lässt die Daten- bzw. IT-Landschaft ein datenschutzkonformes Outsourcing zu?

8 Wird Big Data Analytics genutzt (z.B. Analyse des Kaufverhaltens)?

9 Wird regelmässig überprüft, welche Gesetze und Regulierungen auf die Verarbeitung von (Personen-)Daten anwendbar sind und was dies fürs Unternehmen bedeutet?

10 Besteht eine festgelegte und dokumentierte Datenschutz-Organisation mit definierten Rollen und Verantwortlichkeiten?

11 Wurden Ziele bezüglich Datenschutz und Kontrollmechanismen formuliert?

12 Bestehen unternehmensweite Weisungen bezüglich Aufbewahrung und Vernichtung von (Personen-)Daten und entsprechen diese Weisungen den rechtlichen Vorgaben?

13 Sind Prozesse zum Umgang mit Datenschutzerklärungen vorhanden und umfasst die entsprechende Zustimmungserklärung die datenschutzrechtlichen Voraussetzungen?

14 Werden regelmässig Anpassungen an den internen und externen Datenschutz-Richtlinien/Weisungen/Erklärungen vorgenommen, wenn sich Verarbeitungssysteme, Prozesse geändert haben? Wird generell der Umgang mit dem Datenschutz regelmässig überprüft?

15 Bestehen unternehmensweit einheitliche Prozesse für Zugang, Korrektur und Löschung, wenn ein Kunde eine Anfrage zu seinen Kundendaten stellt?

16 Werden die Auswirkungen von neuen Vorhaben, Produkten, Dienstleistungen und Verarbeitungssystemen auf den Datenschutz proaktiv und konsequent abgeklärt?

17 Decken die Strategie zum Informationsschutz und die entsprechenden Prozesse auch Datenschutzrisiken (z.B. Datenlecks) ab?

18 Ist sichergestellt, dass Dritte, die Personendaten verarbeiten, angemessene technische und organisatorische Schutzmassenehen umgesetzt haben?

19 Werden regelmässig Schulungen zum Datenschutz durchgeführt? Passen diese auf die Verantwortlichkeiten der Teilnehmer?

20 Bestehen unternehmensweit einheitliche Weisungen und Prozesse zum Umgang mit einem Datenverlust oder einem Datenleck?