

# Datenhaltung – wer ist für die Daten verantwortlich?

Daniela Tschol

Jeder Mitarbeitende bearbeitet während seinen geschäftlichen Tätigkeiten Unmengen von Personendaten, speichert sie ab oder schickt sie weiter. Aus Sicht des Managements stellen sich dabei zahlreiche interessante rechtliche Fragen. Nachfolgend werden einige davon aufgegriffen, wie beispielsweise die Zulässigkeit der Datenbearbeitung, die Verantwortlichkeit für die Daten oder gesetzliche Archivierungsvorschriften.

## Bearbeitungsgrundsätze des Datenschutzgesetzes

Die Bearbeitung von Daten ist aus datenschutzrechtlicher Sicht dann relevant, wenn es um Personendaten geht. Personendaten sind alle Informationen, welche eine Aussage über eine bestimmte oder bestimmbare natürliche oder juristische Person machen. Als Bearbeiten gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren. Darunter fällt insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

Gemäss Datenschutzgesetz (DSG; SR 235.1) muss die Bearbeitung von Personendaten zweck- und verhältnismässig sein. Dies hat zur Folge, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, welcher bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich ist oder sich aus dem Gesetz ergibt. Wenn die Bedingung der Zweckmässigkeit erfüllt ist, geht es um die Beurteilung der Verhältnismässigkeit, d.h. die Datenbearbeitung muss geeignet und notwendig sein, um den angestrebten Zweck zu erreichen.

Eine Personendatenbearbeitung ist zudem nur dann zulässig, wenn die betrof-

**Täglich werden im Unternehmen riesige Mengen an Personendaten bearbeitet. Dabei den Überblick zu behalten, welche Daten wo und wie lange vorhanden sind und wer sie bearbeitet, ist extrem schwierig.**

fene Person dazu eingewilligt hat (Vertrag) oder dafür eine gesetzliche Grundlage besteht. Liegt dies vor, so spricht das Datenschutzgesetz von einer zweckmässigen Datenbearbeitung.

Jeder Mitarbeitende darf somit nur diejenigen Daten bearbeiten, welche er für die Erfüllung seiner konkreten Aufgaben benötigt. So ist beispielsweise ein unbeschränkter Zugriff auf sämtliche Daten der Unternehmung für die Erfüllung des Zwecks nicht zulässig. Ein konkret auf die Unternehmensbedürfnisse angepasstes Zugriffs- und Berechtigungskonzept hilft, die Zweck- und Verhältnismässigkeit sicherzustellen.

## Führen einer Datensammlung

Das Führen einer Datensammlung stellt eine Datenbearbeitung im Sinne des Datenschutzgesetzes dar. Als Datensammlung gilt jeder Bestand von Personendaten, welcher so aufgebaut ist, dass Daten nach betroffenen Personen erschliessbar sind.

Wendet man diese gesetzliche Definition auf den Alltag an und schaut sich im Unternehmen etwas genauer um, finden sich zahlreiche Listen, Ordner, Akten oder Register, welche in elektronischer oder physischer Form vorhanden sind. Egal, ob Adresslisten, Geburtstagslisten, Kundenumfragen, HR-Dossiers, Debitoren- und Kreditorenlisten, Forschungsdaten usw., bei all dem handelt es sich um Datensammlungen.

Verantwortlich für die Datensammlung ist diejenige natürliche oder juristische Person, welche über den Zweck und den Inhalt einer Datensammlung entscheidet. In der Regel ist dies das Management, welches somit die datenschutzrechtliche Verantwortung für die Datensammlungen trägt. Damit ist einerseits die Einhaltung

der Datenbearbeitungsgrundsätze gemeint, worunter neben der zweck- und verhältnismässigen Bearbeitung auch die Richtigkeit und Aktualität der Daten fällt. Andererseits zählen beispielsweise aber auch die Verantwortung für Auskunftsbegehren, eine allfällige Anmeldung der Datensammlung, die Massnahmen im Bereich der Datensicherheit usw. dazu.

## Gesetzliche Aufbewahrungsfristen

Buchführungspflichtige Unternehmen sind verpflichtet, die zum Nachweis und Verständnis des Geschäftsergebnisses und der Vermögenslage notwendigen Belege abzulegen und zu archivieren. Neben diesen handelsrechtlichen gibt es insbesondere auch steuerrechtliche Vorschriften, welche den Unternehmen klar vorschreiben, wie und wie lange die Dokumente aufzubewahren sind. Nicht zu vernachlässigen ist auch die Archivierung aus Beweis Zwecken bei drohenden Rechtsstreitigkeiten.

Während die handelsrechtliche Archivierungsfrist grundsätzlich zehn Jahre beträgt, kann sich aus den Spezialgesetzen eine längere Aufbewahrungsdauer ergeben. So verlangt beispielsweise das Mehrwertsteuergesetz (MWSTG; SR 641.20) die Aufbewahrung von bestimmten Belegen im Zusammenhang mit unbeweglichen Gegenständen während 20 Jahren. Die Frist beginnt zudem erst nach dem Ende des Geschäftsjahres oder noch später. Für die Archivierung von nicht mehr bearbeiteten Daten empfehlen sich klare Vorschriften. Zudem gilt es, auch die gesetzlichen Vorschriften (z. B. die Geschäftsbücherverordnung; GeBüV) bezüglich Integrität und Zugriff zu beachten. So muss insbesondere nachvollziehbar sein, ob die Daten nachträglich geändert wurden.



Eine «Radikalkur» – nämlich die Löschung sämtlicher nicht mehr benötigter Daten – ist somit keine Lösung zur Vermeidung von Datenschutzverletzungen.

### Problembereiche in der Praxis

Auch wenn diese theoretischen Ausführungen auf den ersten Blick sehr simpel scheinen, stellen sie in der Praxis häufig ein grosses Problem dar. Für Inhaber von Datensammlungen ist es nämlich sehr verführerisch, mit den vorhandenen Daten mehr zu machen als unbedingt erforderlich. Zudem eröffnet die fortschreitende Technik immer neue Möglichkeiten.

Aber aufgepasst! Über den gesetzlichen Zweck hinausgehende Auswertungen, Verknüpfungen oder auch das Weitergeben innerhalb oder gar ausserhalb der Unternehmung – aus welchen Gründen auch immer – sind meistens unverhältnismässig und somit widerrechtlich.

Es empfiehlt sich deshalb, eine klare interne Struktur und Organisation zu haben, sodass jedem klar ist, welche Daten in welchem Umfang bearbeitet werden dürfen. Eine Zugriffsbeschränkung kann die Datenbearbeitungsvorschriften ergänzen. Werden die Daten zudem regelmässig archiviert, lassen sich unzulässige Datenbearbeitungen weiter minimieren –

und damit zugleich auch mögliche Datenschutzverletzungen vermeiden. Der Zugriff auf diese archivierten Dokumente sollte dokumentiert und aufgezeichnet werden. Entsprechende technische Massnahmen unterstützen dies.

Die Ergreifung solcher Massnahmen liegt in der Verantwortung des Inhabers der Datensammlung und somit in derjenigen des Managements. Und diese lässt sich nicht einfach outsourcen, beispielsweise zusammen mit einem eventuellen Outsourcing der Datenbearbeitung. Der Outsourcer bleibt nämlich für die Datensammlung verantwortlich. Vielmehr müssen in solchen Fällen dem Outsourcing-Partner (Dienstleister) seine Rechte und Pflichten im Umgang mit der Datensammlung überbunden und die Einhaltung dieser Pflichten kontrolliert werden.

### Zusammenfassung

Die Bearbeitung von Personendaten, egal, ob sie natürliche oder juristische Personen betreffen, muss zweck- und verhältnismässig sein. Auch müssen die bearbeiteten Daten richtig und aktuell sein.

Der Inhaber der Datensammlung ist für die Einhaltung der datenschutzrechtlichen Verpflichtungen verantwortlich. Innerhalb eines Unternehmens ist dies in der Regel das Management. Aus Sicht des Managements gilt es deshalb, folgende Fragen zu klären bzw. zu regeln:

- Welche Daten dürfen aus welchem Grund bearbeitet werden (z.B. Gesetz oder Einwilligung)?
- In welchem Umfang dürfen die Daten bearbeitet werden?
- Wer, d.h. welcher Mitarbeitende bzw. welche Stelle, darf welche Daten bearbeiten?
- Wie lange müssen die Daten archiviert werden?

Ein Zugriffs- und Berechtigungskonzept für die Daten unterstützt die Einhaltung der Zweck- und Verhältnismässigkeit.

Die Archivierung von Geschäftsdokumenten und der darin erfassten Informationen dient somit der Sicherstellung einer ordentlichen und nachvollziehbaren Geschäftsführung und damit dem Nachweis der Erfüllung gesetzlicher Vorschriften sowie auch der Beweissicherung für allfällige Rechtsstreitigkeiten. ■