Datenschutz und Datensicherheit: ein Ansatz zur begrifflichen Klärung

Romeo Minini, lic. iur. RA, Exec. MBA HSG

Sprechen Informatikspezialisten, IT-Sicherheitsfachleute und Datenschutzexperten über Datenschutz und Datensicherheit, treten oft Missverständnisse auf. Als wäre das nicht verwirrend genug, wird in der öffentlichen Verwaltung die amtliche Geheimhaltungspflicht der Angestellten im Zusammenhang mit dem Datenschutz ins Spiel gebracht. Der vorliegende Text soll zur Klärung dieser Begriffe beitragen.

Die Menschen haben sehr unterschiedliche Vorstellungen vom Datenschutz. Einigkeit herrscht einzig darüber, dass in der heutigen IT-geprägten Welt die Themen des Datenschutzes allgegenwärtig sind. Einige betrachten den Datenschutz als Abwehr gegenüber staatlichen und privaten Eingriffen in ihre Privatsphäre und glauben, dass ein wirksamer Datenschutz die Menschen vor Persönlichkeitsverletzungen schützt. Andere wiederum sehen im Datenschutz ein Instrument, den technischen Fortschritt aufzuhalten. Unbestritten ist, dass Massnahmen zum Datenschutz einen technischen und finanziellen Aufwand verursachen.

Prinzipiell soll der Datenschutz die Grund- und insbesondere Persönlichkeitsrechte von Personen schützen, über die Verwaltungen oder private Firmen Daten gesammelt haben. In der Schweiz erhielt die Datenschutzgesetzgebung den entscheidenden Impuls denn auch aus der Politik, als es die Fichen-Affäre der 90er-Jahre rechtlich aufzuarbeiten galt. Bis dahin verfügte die Schweiz über ein sehr unvollständiges Datenschutzgesetz. Das Bundesgericht anerkannte im Zuge der europäischen Entwicklungen einzig ein Grundrecht auf informationelle Selbstbestimmung und ein Recht des Einzelnen auf Einsicht, Berichtigung und Löschung von Daten.

Im Zentrum des Datenschutzrechts steht heute der Schutz von Personendaten, namentlich von besonders schützenswerten bzw. sensitiven Personendaten. Dazu zählen beispielsweise Informationen über die Gesundheit, Massnahmen der sozialen Hilfe oder strafrechtliche Verfolgungen. Diesen Daten ist gemeinsam, dass bei einer missbräuchlichen Bearbeitung eine erhöhte Gefahr einer Persönlichkeitsverletzung besteht.

Die Sensibilisierung der Mitarbeitenden für den Datenschutz stellt eine permanente Herausforderung für die Unternehmensführung und die Datensicherheitsverantwortlichen dar. Vor allem in der öffentlichen Verwaltung können Anliegen des Datenschutzes auf taube Ohren stossen, weil Mitarbeitende in der Verwaltung regelmässig auf ihre amtliche Geheimhaltungspflicht hinweisen. Sie sind der Meinung, dass mit der Respektierung dieser Pflicht auch dem Datenschutz entsprochen wird. Dies trifft nicht immer zu. Die Geheimhaltungspflicht hat die Tätigkeit und das Verhalten der Verwaltung gegenüber der Öffentlichkeit oder dem einzelnen Bürger im Blickfeld und ist gegenüber dem Datenschutz

abzugrenzen. Selbst wenn die Geheimhaltungspflicht respektiert wird, kann die verwaltungsinterne Datenbearbeitung gegen den Datenschutz verstossen. Dies ist beispielsweise der Fall, wenn Angestellte Personendaten aus verschiedenen Verwaltungsbereichen wie Steuern, Sozialleistungen, Einwohnerkontrolle usw. ohne gesetzliche Grundlage austauschen. Dann besteht die Verletzung des Datenschutzes nicht in der eigentlichen Fallbearbeitung. Vielmehr wird mit dem verwaltungsinternen Datenaustausch gegen Grundprinzipien des Datenschutzes wie Rechtmässigkeit, Zweckbindung, Verhältnismässigkeit oder Richtigkeit der Datenbearbeitung verstossen. Erfolgt ein Datenaustausch über Personen oder sensitive Daten in einem Umfang und Masse, die für die konkrete Fallbearbeitung weder notwendig noch zweckmässig sind, besteht eine Verletzung nach Datenschutzgesetz. Sobald jedoch die Daten anonymisiert zwischen den Verwaltungsstellen ausgetauscht werden, liegt ein datenschutzkonformes Verhalten vor.

Die Datenschutzgesetzgebung verlangt im Zusammenhang mit der Datensicherheit, dass die Personendaten durch technische und organisatorische Massnahmen in geeigneter und zweckmässiger Weise vor einem unbefugten Bearbeiten zu schützen sind. Es gilt zu gewährleisten, dass die Daten nicht in falsche Hände geraten, unzulässig abgeändert, zerstört oder in missbräuchlicher Weise verwendet werden. Zudem müssen die Daten auch in der Zukunft bestimmungsgemäss bearbeitet werden können.

Bei der Festlegung der konkreten Massnahmen sind anerkannte internationale Normen und Richtlinien zu beachten. Die Massnahmen sind vor allem auf die folgenden Schutzziele auszurichten:

- Vertraulichkeit: Dieses Schutzziel beinhaltet, dass Daten nicht unrechtmässig zur Kenntnis gelangen dürfen. Somit ist sicherzustellen, dass nur berechtigte Personen die Daten einsehen können.
- Integrität: Darunter wird die Richtigkeit und die Vollständigkeit der Daten verstanden.
- Verfügbarkeit: Daten müssen zur Verfügung stehen, wenn sie ordentlicherweise gebraucht werden.
- Authentizität und Nachvollziehbarkeit: Die Datenbearbeitung ist einer Person zuzuordnen. Die Nachvollziehbarkeit setzt voraus, dass Datenveränderungen sowohl erkannt als auch bis zum Urheber nachverfolgt werden können. Zusätzlich ist der Inhalt der Veränderung zu erfassen.

Diese Ziele sind durch technische und organisatorische Massnahmen zu erfüllen. Bei den technischen Massnahmen werden Mittel der Technik verwendet, die periodisch dem aktuellen Stand anzupassen sind. Zu den organisatorischen Massnahmen zählen Vorschriften, Richtlinien, Benutzerweisungen usw. In diesen Benutzerweisungen werden beispielsweise Zuständigkeiten, Arbeitsabläufe oder – im Zusammenhang mit der Dokumentation – die Datenaufbewahrung und Datenarchivierung geregelt.

Die Massnahmen der Datensicherheit sind zudem so auszugestalten, dass die in der Datenschutzgesetzgebung verankerten Prinzipien wirksam und nachhaltig unterstützt werden. Beispielsweise sollen die Zugriffsrechte von Mitarbeitenden so definiert werden, dass sie nur diejenigen Daten bearbei-

ten können, die für die Erfüllung ihrer Aufgaben notwendig sind. Stehen technische und organisatorische Massnahmen zur Auswahl, sind die technischen Massnahmen den organisatorischen vorzuziehen. Die technischen Massnahmen können den gewünschten Sicherheitserfolg unmittelbar herbeiführen. Demgegenüber setzt die Anwendung von organisatorischen Massnahmen stets Zwischenschritte wie etwa den Erlass von Weisungen voraus, bevor die angestrebten Ziele erreicht werden können.

Damit zeigt sich die enge Verknüpfung zwischen Datenschutz und Datensicherheit. Die Massnahmen zur Datensicherheit tragen wesentlich zur Gewährleistung des Datenschutzes bei und richten sich nach dem Schutzbedarf der zu schützenden Personendaten. Bei der Festlegung des Schutzbedarfs stellt sich stets die Frage, welche Auswirkungen die missbräuchliche Verwendung von Personendaten für die betroffene Person hat. Entsteht im Falle einer missbräuchlichen Verwendung von Personendaten und, damit verbunden, einer Datenschutzverletzung eine erhebliche Beeinträchtigung der betroffenen Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen, besteht ein hoher Schutzbedarf. Dieser ist bei besonders schützenswerten oder sensitiven Personendaten regelmässig gegeben.

Fazit

Gilt es in privaten Unternehmen oder in der öffentlichen Verwaltung konkrete Datensicherheitsmassnahmen zu bestimmen, müssen sich die verantwortlichen Stellen in einem ersten Schritt Klarheit über die begrifflichen Grundlagen schaffen. Danach sind die Massnahmen festzulegen, welche die angestrebten Schutzziele optimal erreichen und dem geforderten Schutzbedarf entsprechen. Treten bei der Auswahl der zweckmässigen und verhältnismässigen Schutzmassnahmen Meinungsverschiedenheiten auf, was in der Praxis häufig der Fall ist, sollten die Fachpersonen zusammen mit den Datenschutz- und Sicherheitsverantwortlichen auf konsensualem Weg nach Lösungen suchen. Eine vorgängige begriffliche Klärung der technischen und rechtlichen Grundlagen bildet die notwendige und unerlässliche Grundlage. Die vorliegenden knappen Ausführungen mögen dazu einen Beitrag leisten.