Das Datenschutzmanagementsystem

Von RA lic. jur. Ursula Sury

Wie stelle ich den Datenschutz in meiner Organisation sicher?

Immer mehr Unternehmen befassen sich mit dem Thema Datenschutz. Das Risiko eines Image- und Vertrauensverlustes auf Grund datenschutzspezifischer Vergehen, wollen und können viele Unternehmen nicht tragen. Doch wie schützt man sich und die Daten von natürlichen Personen? Ein wichtiger erster Schritt ist die Dokumentation von Prozessen und Abläufen innerhalb der eigenen Organisation. Dabei stellt sich oft die Frage, wie man ein solches, oft umfangreiches System an Dokumenten und Prozessen organisiert. Hier kommt das Datenschutzmanagementsystem ins Spiel.

Das Datenschutzmanagementsystem

In den vielen Bereichen wie zum Beispiel im Qualitätsmanagement oder in der Informationssicherheit gibt es bereits etablierte internationale Standards, welche zur Entwicklung eines Managementsystems herangezogen werden können. Für das Datenschutzmanagementsystem hat sich bis anhin noch kein solcher Standard durchgesetzt. Jedoch haben sich sogenannte Datenschutzmanagementsysteme, welche sich an den bereits erprobten Disziplinen des Qualitätsmanagements und der Informationssicherheit orientieren, bewährt.

Jedes Unternehmen hat seine eigene Vorstellung, wie seine Aktivitäten und Prozesse gelenkt werden sollen. Bei einem Managementsystem hingen geht es über die operative Betrachtung der Prozesse und Aktivitäten hinaus. Ein Ziel des Managementsystems ist es, eine Evaluierung und Verbesserung der bereits umgesetzten Prozesse anzustreben. Somit unterstützt ein Managementsystem die Umsetzung von Unternehmenszielen. Für spezifische Unternehmensziele gibt es dementsprechend spezifische Managementsysteme. Ein DSMS unterstützt somit primär die Umsetzung der Datenschutzziele des Unternehmens.

Weshalb sollte ein DSMS erstellt werden?

Wie bereits erwähnt, geht es grundsätzlich darum, die Datenschutzziele des Unternehmens zu erreichen. Nebst der Erreichung der Ziele gibt es jedoch noch weitere Aspekte, welche für ein DSMS sprechen.

Ein DSMS ist nebst dem Beleg, dass der Datenschutz in den Prozessen nachgewiesen werden kann, auch ein unterstützendes Tool für den Datenschutzbeauftragten des Unternehmens, um den Anforderungen des Gesetzgebers und der Branche zu entsprechen.

Je nach Grösse eines Unternehmens ist die Abarbeitung der datenschutzrelevanten Anfragen von Kunden oder Behörden in einem «ad-hoc» Prozess zu vollziehen, um an einem Stichtag die Vorgaben zu erfüllen. Dies kann jedoch nur eine Lösung für kleine Unternehmen sein. Mit der Hilfe eines DSMS, worin feste Verantwortlichkeiten sowie klare Strukturen etabliert sind, kann ein kontinuierlicher Verbesserungsprozess (KVP) gestartet werden, welcher die Effektivität des eingesetzten DSMS im Unternehmen fördert. Zudem hilft ein begründetes DSMS die Awareness bei den Mitarbeitern zu verbessern.

DSMS vs. ISMS

An dieser Stelle gilt es, die Unterschiede und Gemeinsamkeiten zwischen einem DSMS und einem Informationssicherheitsmanagementsystem (ISMS) zu beleuchten.

Ein DSMS beschreibt Anforderungen, welche ein ISMS nicht kennt. Dabei muss darauf hingewiesen werden, dass ein ISMS den Fokus auf die internen Assets eines Unternehmens wie Interessen und Vermögensgegenstände legt. Ein DSMS hingegen richtet den Fokus auf die Interessen von Dritten, wie zum Beispiel gesetzliche Vorgaben. Deswegen sollten

bei einem DSMS immer die Anforderungen eines rechtlichen abgesicherten und standardisierten Risiko- und Massnahmenkatalogs berücksichtigt werden. Jedoch muss an dieser Stelle erwähnt werden, dass trotz der inhaltlichen Unterschiede zwischen DSMS und ISMS, ein DSMS die bewährten Komponenten eines ISMS übernehmen sollte.

Ein Beispiel sind die Massnahmen der IT-Sicherheit. Diese unterstützen als wesentliches Werkzeug das DSMS, um die Datenschutzziele eines Unternehmens zu erreichen. Unter Berücksichtigung, dass die beiden Managementsysteme einen unterschiedlichen Fokus haben, ist es in der heutigen Zeit der automatisierten beziehungsweise elektronischen Datenverarbeitung nicht möglich, den Datenschutz ohne IT-Sicherheit zu erreichen. Als Beispiel dazu kann die Protokollierung von Benutzer- und Systemverhalten herangezogen werden. Für die IT-Sicherheit ist eine Aufbewahrung der vollständigen Aktivitätsprotokolle über einen langen Zeitraum kein Problem. In Bezug auf den Datenschutz und das Gesetz sollen die Protokolle jedoch so sparsam wie möglich aufbewahrt werden, um die Prinzipen der Verhältnismässigkeit und der Zweckmässigkeit zu gewährleisten.

Aufbau eines DSMS

Grundsätzlich macht es Sinn, ein DSMS an ein bereits bestehendes Managementsystem anzugliedern, sei es ein Qualitäts- oder Informationssicherheitsmanagementsystem. Beide haben viele Parallelen und somit kann viel Arbeit eingespart werden, wenn man die bereits bestehenden Dokumentationen anreichert oder ergänzt.

Der Aufbau eines DSMS auf ein bereits etabliertes ISMS bietet folgende Vorteile:

- Es gibt bereits einen internationalen Standard mit klaren Vorgaben ISO/IEC 27001.
- Es bestehen auf diesem Standard beruhende Zertifizierungsverfahren.
- Die Auditoren werden jeweils nach der Norm ISO 27006 akkreditiert.
- Der vorhandene Datenschutzbaustein kann bei Bedarf erweitert werden.

Bei der Anreicherung eins bestehenden Managementsystems ist es jedoch wichtig, die Anforderungen an den Datenschutz klar zu definieren, welche sich aus den gesetzlichen Grundlagen und/oder den individuellen Gegebenheiten, welche jedes Unternehmen mit sich bringt, ergeben. Diese Gegebenheiten muss das Datenschutzmanagement berücksichtigen.

Die Erfahrung zeigt, dass die Erarbeitung mithilfe von IT-gestützten Systemen erfolgen sollte. Damit ist sichergestellt, dass der Datenschutz einen starken Bezug zur sich verändernden Technik erhält. Aufgrund der sich stets verändernden Organisation innerhalb der Unternehmen ist das Datenschutzmanagement kein statischer Prozess, sondern muss in einem sich stets überarbeitenden Prozess sichergestellt werden.

DSMS in der Schweiz

Aufgrund der Datenschutz Zertifizierung nach VDSZ des Bundes hat der EDÖB eine Richtlinie herausgegeben, welche Unternehmen die minimalen Anforderungen aufzeigt, welche seitens des Bundes an ein Datenschutzmanagementsystem gestellt werden. Dabei orientiert sich die Richtlinie grundsätzlich am international anerkannten ISO Standard ISO/IEC 27001. Nebst den in ISO erwähnten «controls» müssen unter anderem folgende Kriterien im DSMS behandelt und dokumentiert werden: Rechtmässigkeit, Transparenz, Verhältnismässigkeit, Zweckbindung, Datenrichtigkeit, grenzüberschreitende Datenbekanntgabe, Datensicherheit, Registrierung der Datensammlungen sowie das Auskunftsrecht und Verfahren.

Ob das revidierte Datenschutzgesetz der Schweiz Auswirkungen auf die Anforderungen des Bundes haben wird, muss sich noch zeigen. Die Verordnung zum neuen Datenschutzgesetz wurde noch nicht veröffentlicht.

Fazit

Unternehmen, welche personenbezogene Daten verarbeiten, kommen nicht umhin, sich mit dem Datenschutz zu befassen. Die Erfahrung zeigt, dass eine Erarbeitung eines Datenschutzmanagementsystems sehr sinnvoll ist. Durch ein sich stetig veränderndes Umfeld, verändern sich auch die Anforderungen an den Datenschutz. Ein Datenschutzmanagementsystem kann ein Unternehmen entlasten, in dem die Anforderungen an die Dokumentationen und Prozesse auf strukturierte Weise erfasst und bearbeitet werden können. So können allfällige «ad-hoc» Prozesse vermieden und Struktur in ein komplexes Thema gebracht werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.