Besprechung / Compte rendu

Datenschutz-Managementsysteme im Aufwind?

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

ROLF H. WEBER / FLORENT THOUVENIN (HG.)

Schulthess Juristische Medien AG, Zürich 2016, 194 Seiten, CHF 79, ISBN 978-3-7255-7469-8

Das Buch «Datenschutz-Managementsysteme im Aufwind?» ist ein Tagungsband. Verschiedene, von ausgewiesenen Spezialisten an einer Tagung präsentierte Vorträge wurden darin kompiliert. Inhaltlich zeichnet sich das Werk in zweifacher Hinsicht aus: einerseits durch seinen Fokus auf für die Unternehmenspraxis relevante Themen, andererseits durch verschiedene Beiträge ausgewiesener Spezialisten aus der Advokatur, Unternehmenspraxis und Wissenschaft.

Die im Zentrum stehenden «Datenschutz-Managementsysteme» *(DSMS)* bezeichnen *klar definierte Vorgehensweisen, mithilfe deren sich Datenschutzkonformität in Geschäftsprozesse integrieren lässt*. DSMS werden denn auch in der neuen Datenschutzgrundverordnung der EU *(DSGV)* als Unternehmenserfordernis wörtlich erwähnt. Undeutlich verbleibt aber die konkrete Ausgestaltung solcher Systeme. Diverse Aspekte können ihren Beitrag für ein DSMS schaffen, wie zum Beispiel das Festlegen von Zugriffsrechten, die Protokollierung von Datenzugriffen, die Anonymisierung und sichere Aufbewahrung von Daten sowie das Anlegen eines Lebenszyklus für Daten (d.h., dass z.B. eine Zweckbindung für die Nutzung an Daten «angeheftet» wird, sodass diese automatisch zweckkonform bearbeitet oder dereinst wieder gelöscht werden).

Das Buch gliedert sich in sieben Beiträge: In einem ersten Beitrag befasst sich DAVID ROSENTHAL mit dem Thema *Datenschutz-Compliance in Unternehmen*. Nach seiner Auffassung besitzen die meisten Unternehmen kaum Erfahrung mit dem Datenschutz und benötigen eine etappenweise Instruktion. Als wichtigste Bausteine zur Etablierung von Datenschutz-Compliance schlägt ROSENTHAL verschiedene Einzelschritte vor. Bei der Datenschutz-Compliance seien Risikoentscheide notwendig, d.h. eine Fokussierung von Ressourcen und Compliance auf jene Aspekte, die prioritär wichtig sind. Er schlägt in einem ersten Schritt die gesamtheitliche Aufnahme von Missständen in einem Unternehmen anhand eines *12-Fragen-Katalogs* vor. Zu unterscheiden seien dabei

– formale Datenschutzerfordernisse (wie zum Beispiel Notifikationen und Registrierungen bei Behörden),
– materielle Restriktionen (wer welche Daten wie und wann bearbeiten darf) sowie
– die Governance (d.h. Vorkehrungen, um materielle und formale Erfordernisse sicherzustellen, wie etwa der Erlass von Richtlinien, Schulungen, Dokumentationen).

ROSENTHAL empfiehlt, einen gewissen Leidensdruck gegenüber Unternehmen aufzubauen. So ist Unternehmen zu erklären, dass die Datenschutzaufsicht in der Schweiz nicht flächendeckend arbeitet, sondern aufgrund ihrer beschränkten Ressourcen einzelne Unternehmen auswählt, gegen die sie dann aber mit aller Härte vorgeht. Unternehmen müssen auch darauf sensibilisiert werden, dass die EU soeben ihr Datenschutzrecht revidiert und in vielen Bereichen verschärft hat und dies auch extraterritoriale Auswirkungen auf gewisse Unternehmen in der Schweiz haben kann. Fehlende Compliance mit der DSGV kann Verwaltungsstrafen bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes mit sich ziehen. Weiter rät ROSENTHAL zur Etappierung datenschutzrechtlicher Korrekturmassnahmen: Die Erfahrung zeigt, dass ambitionierte (Gross-)Datenschutzprojekte in den meisten Fällen nicht richtig realisiert werden. Eine nachhaltige Datenschutzkultur lässt sich in einem Betrieb auch

nicht mit Weisungen oder Aktivismus erzwingen, sie ist nur bei einer Sensibilisierung und entsprechender Umsetzung im Alltag gewährleistet. Hat sich eine (Teil-)Massnahme erst einmal im Konzern etabliert, kann sie viel einfacher auf andere Bereiche ausgedehnt werden. Schliesslich rät der Autor zu einer interdisziplinären Vorgehensweise: DSMS müssen intern umgesetzt werden können. Als wirkliche Herausforderungen erweisen sich somit die Kenntnis interner Verhältnisse und der Umgang mit innerbetrieblichen «Stakeholdern». Zuletzt empfiehlt ROSENTHAL «Mut zur Lücke»: DSMS sollten nicht danach streben, alle Anforderungen des Datenschutzes abzudecken, sondern sich auf essenzielle Punkte beschränken. Dies hat den nützlichen Nebeneffekt, dass eine innenpolitische Unterstützung leichter zu bewerkstelligen ist. Das Ziel von DSMS sei letztlich v.a., dass Datenschutz in einem Unternehmen nicht mehr nur ad hoc bzw. reaktiv, sondern möglichst systematisch und proaktiv betrieben wird.

Im zweiten Beitrag befasst sich PROF. DR. ROLF H. WEBER mit internationalen Trends zu DSMS. Dabei wird eine konzeptionelle Einordnung von DSMS vorgenommen. Als konzeptionelle Grundelemente herauskristallisiert werden

– organisatorische Regeln,
– unternehmensinterne Datenschutzstrategien,
– Projektmanagement,
– Datenklassifizierungsregimes,
– Verantwortlichkeiten und Anforderungen für Kontroll- und Überwachungsprozesse sowie
– Compliance (d.h. die Kontrolle der Einhaltung datenschutzrechtlicher Regeln).

WEBER erörtert sodann historische Vorläuferkonzepte von DSMS. Dazu gehört das zwischenzeitlich oft verwendete Schlagwort *«Privacy by Design»* oder die von der Europäischen Union bereits früher verwendete Empfehlung des *«Privacy Impact Assessment».* Gemäss diesen Begriffen ist jedes Unternehmen mit besonderen Datenrisiken konfrontiert, die es notwendig machen, spezifische Schutzvorkehrungen in Betracht zu ziehen. Gemäss WEBER erweist es sich als sachgerecht, externe Experten beizuziehen, um eine Unabhängigkeit von Risikoeinschätzungen zu gewährleisten. Im Weiteren liefert WEBER einen Überblick über international (privat-)normierte DSMS. Sowohl das Model der «International Association of Privacy Professionals», das «Privacy Accountability Framework» des privaten Unternehmens Nymity Inc. wie auch das «Privacy Management Program» des Datenschutzbeauftragten von Hong Kong werden beleuchtet. Während einige dieser DSMS den Fokus mehr auf den Datenschutzlebenszyklus legen, betonen andere wiederum stärker die Sicherheitsanforderungen und die individuellen Rechte der Betroffenen. Zuletzt widmet sich der Autor der rechtlichen Verankerung von DSMS in der Europäischen Union. Gemäss der neuen DSGV müssen datensammelnde Unternehmen bereits in der Planung der Datenbearbeitung die Erfassung personenbezogener Daten auf ein Minimum beschränken und sicherstellen, dass diese nur für die spezifisch festgelegten Zwecke bearbeitet werden. Art. 38 der DSGV eröffnet zudem die Möglichkeit, Verhaltensstandards der Industrie in die Beurteilung der Eignung eines DSMS miteinfliessen zu lassen. In diesem Zusammenhang betont WEBER, dass die Nichteinhaltung von internen Regeln und Kontrollmechanismen stets zu einer Sanktion führen sollte, denn notwendig sei die Verwirklichung des Prinzips der «Accountability». Zuletzt liefert WEBER einen Ausblick auf Selbstregulierungswerke unterschiedlicher Branchen. Auch diese können nämlich geeignete Grundlagen für DSMS bilden, wenngleich ohne eine normative (Gesetzes-)Wirkung. Darunter fallen insbesondere die Rahmenwerke COSO, COBIT, die Zertifizierungen ISO 9001, 20000, 27000 sowie das Rahmenwerk ITIL. WEBER prognostiziert, dass sich im europäischen Markt neue Anbieter von DSMS etablieren könnten, die massgeschneiderte Branchenlösungen anbieten. WEBER mahnt indes zu Vorsicht: Ein softwarebasiertes DSMS könne nicht sämtliche Datenschutzprobleme selbständig lösen. Vielmehr bleibe ein Zusammenspiel von Technologie, innerbetrieblichen Abläufen und menschlich gesteuerten Interessenabwägungen erforderlich, um ein optimales und in sich geschlossenes DSMS zu verwirklichen.

In einem dritten Beitrag untersucht NICOLE BERANEK ZANON die wichtigsten formalen Eckpunkte von DSMS, anders als im vormaligen Beitrag von WEBER nun aber vornehmlich aus schweizerischer Sicht. Dreh- und Angelpunkt ihres Beitrages liegt in Art. 22 Ziff. 1 der Verordnung zum Datenschutzgesetz *(VDSG).* Gemäss dieser Bestimmung muss ein Dateninhaber stets zum Nachweis gesetzeskonformer

Datenbearbeitungen in der Lage sein. Insofern kommt DSMS nicht nur eine unternehmerische Dimension, sondern auch eine Beweissicherungsfunktion zu. Als von besonderer Bedeutung in diesem Zusammenhang erweist sich nicht nur die VDSG, sondern auch zugehörige Richtlinien und ISO-Normen. All diese Normwerke liefern spezifische Vorgaben zur Datenbearbeitung. Die Autorin geht dabei insbesondere auf die unter Art. 11 Abs. 2 DSG erlassene Richtlinie des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten *(EDÖB)* über die Mindestanforderungen an ein Datenschutzmanagementsystem *(REDMS)* ein. Die REDMS orientiert sich stark an den internationalen Normen ISO 27001: 2013, ISO 27002: 2013 und ISO 9001. Gemäss REDMS genügt ein Datenschutzmanagementsystem den Mindestanforderungen, wenn es diese referenzierten, internationalen Regelwerke grundsätzlich einhält. Als hilfreich zusammengefasst erweisen sich die 20 vom EDÖB konkret empfohlenen Umsetzungsmassnahmen zur Datensicherheit. Aus diesen geht hervor, wie Datenschutzüberlegungen in die konkrete Projekt- und Managementplanung eines Unternehmens (im Sinne einer Best Practice) einfliessen können.

Gleich anschliessend knüpft MARIA WINKLER mit ihrem Beitrag zum Thema Datenschutzzertifizierungen an. In ihrem Beitrag geht die Autorin genauer auf das freiwillige Selbstregulierungskonzept einer Datenschutzzertifizierung gemäss Art. 11 DSG ein. Unternehmen steht es frei, unternehmensinterne Prozesse zertifizieren zu lassen. Zertifiziert werden können alle oder einzelne, abgegrenzte Datenbearbeitungsprozesse, für die ein Unternehmen verantwortlich ist. Im Gegensatz zum Ausland ist eine Datenschutzzertifizierung von «Produkten» – im Sinne eines Qualitätszeichens für deren Vermarktung – gesetzlich nicht vorgesehen. Von der Freiwilligkeit einer Datenschutzzertifizierung sind wohlgemerkt Krankenversicherer in der Schweiz ausgeschlossen. Krankenversicherer müssen nämlich für den Empfang von Fallpauschalenrechnungen nach dem Tarifsystem SwissDRG über eine zertifizierte Datenannahmestelle verfügen. Auch WINKLER analysiert die VDSG und die REDMS mit Verweis auf internationale ISO-Normregelwerke. Hilfreich am vorliegenden Aufsatz erweist sich die systematische Übersicht einzelner Schritte einer Datenschutzzertifizierung. Als wichtigste Determinanten erweisen sich

– die Dokumentation der zertifizierungsrelevanten Prozesse,
– die Einhaltung rechtlicher Anforderungen (insbesondere die neun Ziele in der VDSG und die 20 vom EDÖB vorgeschlagenen Massnahmen),
– die Einhaltung der Datensicherheitsanforderungen (mit Weiterverweis auf einschlägige ISO-Normen, wobei zu jeder im EDÖB-Leitfaden erwähnten Massnahme des Anhangs A eine «Anwendbarkeitserklärung» zum zertifizierten Bereich erfolgen muss),
– jährliche Wiederholungen des Audits und eine entsprechende Dokumentation, andernfalls eine Sistierung oder schlimmstenfalls sogar ein Entzug des Zertifikats durch die Zertifizierungsstelle stattfinden kann.

Als nächste Autoren widmen sich FLORENT THOUVENIN und JUTTA SONJA OBERLIN der *Überwachung der Durchsetzung von Datenschutzmanagementsystemen*. Der Fokus des Beitrags liegt damit mehr auf dem verwaltungsrechtlichen Aufsichtskonzept im klassischen Sinne und weniger auf der unternehmensinternen Implementierung eines DSMS. Eine solche Aufsicht kann durch die Zertifizierungsstelle selbst oder – ergänzend – durch den EDÖB erfolgen. Während erstere Aufsicht sich darauf beschränkt, die Voraussetzungen der Zertifizierung (und insbesondere die jährliche Re-Evaluation und Dokumentierung) zu prüfen, widmet sich der EDÖB in seiner allgemeinen Aufsichtstätigkeit dem Prüfen der Einhaltung gesetzlicher Vorschriften. THOUVENIN/ OBERLIN erläutern auch die Rechtsmittelwege, sofern ein Unternehmen mit konkreten Empfehlungen des EDÖB nicht einverstanden sein sollte. Kritisch hervorgehoben wird die in Art. 10 Abs. 1 VDSG vorgesehene Frist von 30 Tagen, innert deren ein von der Zertifizierungsstelle diagnostizierter Mangel vom Unternehmen zu beheben ist. Zu Recht erwähnen die Autoren, dass diese Frist sich als äusserst kurz erweist, wenn man sich die damit verknüpfte Androhung einer Sistierung oder Entziehung der Zertifizierung vor Augen hält.

In einem weiteren Beitrag untersucht der Autor URS PELZER das rein selbstregulatorische Datenschutz-Gütesiegel «GoodPriv@cy». Dieses ist aus der Zusammenarbeit der Schweizerischen Vereinigung für Qualität- und Management-Systeme *(«SQS»)* und weiteren Partnerfirmen entstanden. Die Marke «GoodPriv@cy» ist seit dem 1. März 2000 beim Eidgenössischen Institut für geistiges Eigentum mit einem dazugehörigen Markenreglement hinterlegt. Die datenschutzrechtlichen Anforderungen

von GoodPriv@cy sind hingegen im Regulativ Datenschutzmanagementsysteme GoodPriv@cy festgehalten. Das Zertifizierungsverfahren ist eng an die internationale Norm ISO 9001 angelehnt. Dies erlaubt es, eine Zertifizierung auch mit den Anforderungen aus ISO 27001 zu ergänzen. Zertifizierungsstelle für GoodPriv@cy sind die SQS sowie Partner im International Certification Network IQNet. GoodPriv@cy hat sich bis heute nicht als Erfolgsmodell bewährt. PELZER führt dies auf Irritationen im Markt zur gesetzlichen Datenschutzzertifizierung zurück und ist der Auffassung, dass Garantiemarken wie GoodPriv@cy gegenüber internationalen Standards oder der VDSZ und den EDÖB-Richtlinien – die als «Behörden-Gütesiegel» verstanden werden – benachteiligt sind. Dennoch erweisen sich die bis heute knapp 60 GoodPriv@cy-Zertifizierungen verglichen mit den nur 9 Zertifizierungen nach VDSZ/EDÖB-Richtlinie, die dem EDÖB gemäss Art. 11a Abs. 5 lit. f DSG gemeldet wurden, als respektabel. In einem abschliessenden Resumé befindet PELZER, dass sich Datenschutzgütesiegel bislang in der Schweiz (sei es nun auf privater oder gesetzlicher Basis) noch nicht stark durchgesetzt haben. Dennoch ist PELZER überzeugt, dass die Umsetzung des Datenschutzes auf Grundlage eines «Managed Privacy»-Qualitätsmanagements langfristig der einzige nachhaltige und effiziente Ansatz ist.

Den Abschluss dieses Sammelwerkes liefern DOMINIQUE N. STAIGER und ROLF H. WEBER mit ihrem Beitrag zu *Datenschutzmanagementsystemen in der Cloud.* Der Beitrag erweist sich als eine gute und zeitgemässe Abrundung, zumal zahlreiche Unternehmen vermehrt externe Cloud-Dienste zur Abspeicherung und Bearbeitung ihrer Daten in Anspruch nehmen. Die Anforderungen an ein DSMS für Clouds nutzende Unternehmen sind akzentuiert, zumal sich auch Cloud-spezifische Herausforderungen an ein DSMS stellen. Ein kritischer Aspekt ist in der territorialen Dimension von Cloud-Diensten zu sehen. So ist weitgehend bekannt, dass die USA einen zumindest aus Schweizer Sicht nicht adäquaten Datenschutzstandard gewährleisten können. Nach Auffassungen von STAIGER/WEBER ist deshalb tunlichst zu vermeiden, Daten an US-amerikanische Cloud-Anbieter zu übermitteln. Auch bei europäischen Cloud-Anbietern bestehe keine Sicherheit, zumal unter Umständen ein US-amerikanisches, verbundenes Konzernunternehmen von einem Gericht aufgefordert werden könne, in Europa bei einer Tochtergesellschaft belegene, doch für das US-amerikanische Unternehmen zugängliche Daten zu editieren. STAIGER/WEBER nehmen dabei Bezug auf ein im Verfassungszeitpunkt noch nicht rechtskräftiges New Yorker Gerichtsurteil, welche das Unternehmen Microsoft Inc. zur Herausgabe von Daten, die auf einem irischen Server lagen, verurteilte. Der Autor erlaubt sich, hier zu ergänzen, dass jenes Urteil unterdessen höchstrichterlich aufgehoben und Microsoft von einer Datenherausgabe aufgrund der «Extraterritorialität» des Editionsbegehrens befreit wurde. Dieses Urteil verbleibt in der Lehre denn auch umstritten. Abgesehen von den für Cloud-nutzende Unternehmen relevanten Pfeilern eines DSMS heben die Autoren folgende Zusatzaspekte hervor: Einerseits ist eine Verschlüsselung oder Anonymisierung von in die Cloud übermittelten Daten anzuvisieren. Dies kann intern beim auslagernden Unternehmen stattfinden (via DSMS-Software), andererseits bieten auch Cloud-Anbieter eigene verschlüsselte Übermittlungskanäle via Schnittstellen (sog. «Homomorphic Functions»). Zudem bieten Cloud-Anbieter bisweilen eigene DSMS-Software für Kunden im Rahmen ihres Cloud-Angebots an. Damit kann ein Kunde die konkrete Zuweisung und Nutzung von Daten innerhalb der Cloud vollautomatisch steuern. Sogenannte «Präferenzsysteme» können dem Kunden dabei erlauben, seine Daten in Kategorien zu unterteilen und dem Cloud-Anbieter so vorzugeben, wie er mit diesen alsdann verfahren darf. Schliesslich weisen die Autoren auf die herkömmlichen vertraglichen Sicherungsinstrumente gegenüber Cloud-Anbietern hin (z.B. die starken Kontroll- und Auditrechte gegenüber Anbietern und idealerweise auch seinen Subunternehmern sowie die Pflicht des Anbieters zur Meldung von datenschutzverletzenden Vorfällen etc.). Hier ist nach Auffassung des Autors mit Interesse zu erwarten, ob Cloud-Anbieter inskünftig bereit sein werden, ihre – doch eher standardisierten – Cloud-Dienstleistungen in einer auf Kunden massgeschneiderten Weise anzubieten oder sogar individuell zu verhandeln.

Das Werk schliesst zuletzt mit einer Zusammenfassung der an der Tagung erfolgten Podiumsdiskussion geleitet durch DOMINIK N. STAIGER.

Das rezensierte Sammelwerk liefert einen vielseitigen Überblick über die unternehmerische Dimension von DSMS. Sämtliche Autoren des Werks sind ausgewiesene Experten und analysieren die Thematik aus unterschiedlichen Blickwinkeln. Aufgrund des kompilierten Sammelwerkcharakters sind gewisse Überschneidungen und Redundanzen zwischen den individuellen Einzelbeiträgen teilweise erkennbar. Dennoch beleuchtet jeder Beitrag verschiedene Aspekte von DSMS. Die konkrete Umset-

zung von DSMS bleibt indes eine praxisbezogene Herausforderung, welche Unternehmensverantwortliche, Techniker, Inhouse-Counsels sowie extern herbeigezogene Rechtsanwälte während der nächsten Jahre gemeinsam erarbeiten und weiterentwickeln werden müssen. Das Buch liefert dazu wertvolle Impulse und ist Lesern aus der Unternehmenspraxis deshalb sehr zu empfehlen.

Dirk Spacek, Dr. iur., LL.M., Rechtsanwalt, Zürich