Martin Rost

Datenschutzmanagementsystem

Dieser Artikel umreißt ein Datenschutzmanagementsystem, bei dem das Standard-Datenschutzmodell mit wesentlichen Komponenten des Informationssicherheitsmanagements nach ISO 27001 kombiniert wird.

1 Einleitung

Unter der Geltung des Datenschutzrechts und seiner verfassungsrechtlichen sowie europarechtlichen Grundlegungen muss eine Daten verarbeitende Organisation nachweisen können, dass sie die von ihren Geschäftsprozessen betroffenen Personen nicht über das grundrechtlich hinnehmbare Maß hinaus fremdbestimmt.[1] Dieser Artikel verfolgt den Ansatz, standardisiert-automatisierten Organisationsprozessen ebenso standardisiert-automatisierte Prozesse der Datenschutzkontrolle an die Seite zu stellen. Für die handlungspraktische Führung dieses Nachweises benötigt die Organisation ein Datenschutzmanagementsystem (DSMS). Ein DSMS unterstützt somit im Wesentlichen die Aufgaben eines Datenschutzbeauftragten (DSB).

Das DSMS soll eine Organisation in die Lage versetzen, eine systematische Planungs-, Kontroll-, Eingreif- und Unterstützungsfunktion über die eigene Datenschutzkonformität selbst auszuüben, – und zwar in standardisierter und möglichst maschinell gestützter Form.

Ein DSMS beschreibt einen Typ von Anforderungen, den ein Informationssicherheitsmanagementsystem (ISMS) nicht kennt. Ein ISMS dient unmittelbar dem Schutz der eigenen Interessen und Vermögensgegenstände (*assets*) einer Organisation. Ein DSMS nimmt dagegen von vornherein den Blick auch auf die Interessen Dritter, vergleichbar der Einhaltung von Vorgaben der Umwelt- oder der Wirtschaftsaufsicht. Deshalb empfiehlt es sich, einen rechtlich abgesicherten und standardisierten Risiko- und Maßnahmenkatalog zu übernehmen. Dieser Katalog wird nachfolgend aus dem Standard-Datenschutzmodell bezogen.

Ein DSMS soll zum einen die Transparenzanforderungen an Organisationen erfüllen. Im Außenverhältnis von Organisationen gegenüber Personen unterstützt es deshalb aktiv das Informationsbedürfnis organisationsfremder Personen, die Auditiertätigkeiten interner Prüfer sowie die Prüftätigkeiten externer Aufsichtsbehörden. Außerdem sollte ein DSMS Techniken betreuen, mit deren Hilfe Betroffene ihre Daten in Organisationen managen können. Und es sollte Infrastrukturen unterstützen, mit denen die Zweckbindung einer Datenverarbeitung technisch durchgesetzt wird. Dieser Aspekt umfasst bspw. Infrastrukturen, die im Rahmen des (nutzerkontrollierten) Identitätenmanagements entwickelt wurden. Diese Techniken und Infrastrukturen versetzen Organisationen in die Lage, sowohl mit gesicherten Identitätsattributen, die bspw. dem Neuen Personalausweis entnommen werden, als auch mit Rollenpseudonymen oder anonymen Credentials umzugehen, wenn dies Abwicklung von Interaktionen zwischen Organisationen und Personen funktional hinreicht.[2] Und nicht zuletzt sollte ein DSMS den Prozess des datenschutzrechtlichen Beurteilens von Verfahren initiieren und den Sachstand verfolgbar machen können.

Ein ISMS legt die systematische Behandlung rechtlicher Anforderungen, wie denen des Datenschutzrechts, nur insofern nahe, als dass die Risiken eines Compliance-Verstoßes aus der Sicht der Geschäftsprozesse zu beurteilen sind. Anders als ein DSMS ergreift ein ISMS nicht qua Infrastruktur Partei für die Betroffenenrechte. DSMS und ISMS stehen in dieser Zuspitzung sowohl in einem einander unterstützenden als auch gegenläufigen Verhältnis der Umsetzung von Anforderungen an personenbezogene Verfahren. Und dieser Unterschied sollte in der aktuellen Diskussion eher betont als verwischt werden.

Ein DSMS sollte trotzdem die Nähe zu einem ISMS sowie zu den anderen etablierten Prozessframeworks suchen, wie bspw. ITIL, CoBIT oder Methoden des Qualitäts- und Finanzmanagements und der Revision. Denn das ist eine Voraussetzung dafür, dass Datenschutzmanagement zu einem selbstverständlichen Teil einer Organisation werden kann. Ein DSMS muss dabei so mächtig ausgelegt sein, dass es Frameworks, die latent etwa an einer Leistungskontrolle von Mitarbeitern interessiert sind, und ISMSe, die latent eine Verhaltenskontrolle von Mitarbeitern nahelegen, auf Grundrechtskonformität zu überprüfen vermag. Trotz der inhaltlich zu bewahrenden Distanz zwischen DSMS und ISMS kann ein DSMS aber bewährte Komponenten eines ISMS übernehmen.

Eine solche, von Verfassungs- und Europarechts wegen aufgegebene, Prüftätigkeit gegenüber etablierten Frameworks und ISMSen tatsächlich auszuüben ist gerade auf der Ebene organisatorischer Maßnahmen jedoch noch keine Praxis. Im Unterschied et-

1 Ich danke Kirsten Bock und Wolfgang Zimmermann für die gewogen kritische Kommentierung.

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz" beim Unabhängigen Landeszentrum für Datenschutz (ULD) in Kiel.

E-Mail:
martin.rost@datenschutzzentrum.de

2 Ein nutzerkontrolliertes Rollenpseudonym erlaubt einer Person, Reputation für einen Teil ihrer Identität , bspw. in der Berufsrolle, im Prinzip ein Leben lang zu pflegen.. Es obliegt dann allein der Person, ob sie das Pseudonym aufdeckt oder nicht. Die Schutzwirkung eines Rollenpseudonyms ist als nicht besonders hoch einzuschätzen, weshalb bei hohen Schutzanforderungen eher Transaktionspseudonyme oder anonyme Credentials zum Einsatz kommen, die jeweils nur für eine Transaktion genutzt werden (vgl. Hansen / Pfitzmann 2011).

wa zu IT-Grundschutz wurden bislang keine vergleichbaren Standards bzgl. der Prüfung technisch-organisatorischer Datenschutzmaßnahmen, geschweige denn Risikoindikatoren zur Messung der Wirksamkeit von Maßnahmen herausgebildet. Die Datenschützer haben sich, so scheint es, bislang zu sehr auf den Druck gesetzlicher Anforderungen verlassen. Und weil IT-Sicherheit die Beherrschbarkeit, Robustheit und Vertrauenswürdigkeit der Datenverarbeitungsverfahren in Organisationen verbessert, kann es selbst professionellen Datenschützern unterlaufen, den eigenständigen Beitrag eines DSMS gering zu schätzen. Die Folge davon ist, dass das Motiv der IT- bzw. Informationssicherheit das des Datenschutzes dominiert.[3]

2 Zum Stand der Diskussion zu DSMS

In einer Handreichung zu „Datenschutzmanagement" aus dem Jahre 2002 findet sich, neben einer Aufstellung an Aktivitäten, die ein DSB gemäß BDSG zu erfüllen hat, ein Abschnitt zu Prozessaspekten unter der Maßgabe, dass „die Datenschutzüberwachung in die Qualitätssicherung zu integrieren" sei (ULD 2002). Wenige Jahre später wird diese Aufstellung durch eine Sammlung von Aufklärungs- und Awareness-Artikeln und praxisgestählte Checklisten für Datenschutzbeauftragte ergänzt (Kongehl et al. 2006). Wiederum wenige Jahre später wurde vorgeschlagen, den PDCA-Zyklus[4] als zentrale Prozesskomponente eines DSMS zu nutzen (Looman/Matz 2010). Rund zwei Jahre später liegt ein Vorschlag mit identifizierten Musterprozessen des Datenschutzmanagements vor, der bereits Bezug auf die sechs „elementaren Schutzziele" des Datenschutzes nimmt (Prietz 2012). Anfang März 2013 setzt die Holländische Datenschutzaufsichtsbehörde eine Richtlinie in Kraft, deren Gesetzesartikel direkt Bezug auf die Phasen des PDCA-Zyklus nehmen, ein Privacy-Impact-Assessment vorsehen, eine Risikoanalyse integriert haben und sich generell an der ISO270xx-Familie orientieren, wobei die Risiken unmissverständlich aus der Betroffenenperspektive formuliert sind (CBP 2013: 20).

Während die beiden erst genannten Vorschläge Anforderungen und konkrete Maßnahmen versammeln, diese aber nicht zu einem Management*system* im Sinne aufeinander abgestimmter Daten, IT-Systeme und Prozesse systematisieren und verdichten, bietet der Vorschlag von Looman/Matz zwar ein systemisches Managementmodell, aber keinen überzeugenden Bezug zu den wesentlichen Bestimmungen des Datenschutzrechts sowie zu den spezifischen technisch-organisatorischen Datenschutzmaßnahmen, wie sie bspw. im Rahmen der „Privacy-Enhancing-Technologies" (PET) oder des „nutzerkontrollierten Identitätenmanagements" entwickelt wurden. Diese Kritik gilt auch für den Vorschlag der CBP, der aber immerhin die internationalen Entwicklungen beachtet und entschieden die Betroffenenperspektive einnimmt. Im Vorschlag von Prietz gelingt es zwar, über den Rückgriff auf die sechs elementaren Schutzziele den Bezug zum Datenschutzrecht herzustellen, allerdings ist keine Systematik bzgl. des Zusammenhangs der Managementprozesse ersichtlich.

Die Idee, DSM an den PDCA-Zyklus zu koppeln oder umfassender noch an ein ISMS anzulehnen, ist nicht neu. Sie wurde bereits vor der Verabschiedung der ISO 27001, die 2005 im Wesentlichen aus den British Standards BS 7799-2:2002 hervor ging, formuliert (vgl. Meints 2007). Die ISO 27001 erlangte in Deutschland Bedeutung insbesondere in der Verbindung mit Maßnahmen nach IT-Grundschutz (vgl. Meints 2006; BSI-ISOGS, o.J.). In diese Tradition stellt sich im Grundsatz auch dieser Beitrag. Allerdings mit dem wesentlichen Unterschied, die bewährten systematischen bzw. methodischen Aspekte der ISO 27001 zu übernehmen und die Inhalte auf die spezifischen Anforderungen des Datenschutzes hin umzuarbeiten. Der dezidierten Informationssicherheitsperspektive, die bspw. Meints eingenommen hat, gilt ein DSM nur als Anhängsel eines ISMS, wonach die personenbezogenen Daten lediglich noch ein wenig aufwändiger zu sichern sind als andere Unternehmensdaten. Dabei ist es grundrechtlich geboten, dass ein DSMS ein ISMS auf Datenschutzkonformität hin kontrolliert.

In einem Beitrag von Quring-Kock (2012) zur Debatte wird der Unterschied zwischen ISMS und DSMS auf technisch-organisatorischen Ebene zwar nicht hinreichend trennscharf benannt, aber es wird vollkommen zu Recht empfohlen, sich auf die Herausbildung von ISMSen in Organisationen zu konzentrieren, bis endlich überzeugende Konzepte zu einem DSMS vorliegen. Unnötigerweise wird dann aber vorgeschlagen, ISMS und DSMS zu integrieren, mit dem Argument, dadurch Mehrfacharbeit zu vermeiden. Dem möchte der Autor in unmittelbarer Entgegnung wie folgt widersprechen:

Datenschutz setzt IT-Grundschutz nicht unbesehen voraus. Vielmehr verlangt IT-Grundschutz ebenfalls eine stetige, also am besten durch ein DSMS unterstützte, Prüfung auf Vereinbarkeit mit Datenschutzrecht. Die anhand der Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit getroffenen Maßnahmen der Informationssicherheit müssen insofern im Hinblick auf die spezifischen Schutzziele der Transparenz, Intervenierbarkeit und Nichtverkettbarkeit profiliert werden. Datenschutz wird im IT-Grundschutz nach BSI und in der ISO 27001 konzeptionell nachrangig, und ohne Berücksichtigung spezifischer Datenschutz-Maßnahmen, abgehandelt. Nicht die Integration sondern die Separation eines DSMS von einem ISMS ist geboten. Und es wäre logisch, dann auch den ohnehin nur optionalen Maßnahmenteil zum Datenschutz aus dem Grundschutzkatalog herauszunehmen.[5]

3 SDM und ISO 27001

Die im Wesentlichen zu beantwortende Frage eines Konzepts zu DSMS besteht darin, was ein Datenschutzmanagementsystem, insbesondere auf der Ebene der technischen und organisatorischen Maßnahmen, steuern und regulieren soll. Diese Frage kann mit Hilfe von Anforderungskatalogen an DSBe (Kongehl 2006) sowie dem Standard-Datenschutzmodell (SDM) beantwortet werden (Rost 2012). Erst dann stellt sich die Frage nach dem Wie des Regelns. Und hier lautet der zweite Vorschlag, es mit den

3 Es zeichnet sich ab, dass für die Anliegen der Informationssicherheit eigene Rechtgrundlagen geschaffen werden und somit für die Umsetzung von Datenschutzrecht über IT-Sicherheit kein operativer Anker mehr besteht. Wenn die Datenschützer dann operativ und methodisch nichts Eigenes zu bieten haben, wird sich die Beachtung des Datenschutzrechts, trotz der fortgesetzt bestehenden Gesetzeslage, auch im öffentlichen Bereich weiter verringern (vgl. Rost 2013).

4 Plan-Do-Check-Act, mehr dazu weiter unten.

5 Allerdings können sich die Datenschützer die Folgen einer solchen Separation strategisch nur dann leisten, wenn sie zuvor methodisch auf Augenhöhe mit IT-Grundschutz gleichzögen.

wesentlichen Prozesskomponenten aus der ISO 27001 zu versuchen (Kersten et al. 2011)[6].

Der nachfolgende Versuch kann dieses Zusammenspiel von SDM und ISO 27001 nur umreißen. Ein hinreichend ausgearbeitetes Datenschutzmanagementsystem erforderte – neben vielen Festlegungen im Detail, für die hier ohnehin kein Platz besteht – zumindest die Durchsicht weiterer Standards wie bspw. die der ISO 27002-27005, ISO 29100 („Privacy Framework") und die ISO 29101 („Privacy Architecture")[7] 31000 oder auch die der 9000er Familie.

Und noch etwas ist kurz anzusprechen: Während bei einem ISMS der Sicherheitsbeauftragte für die Sicherstellung des Betriebs verantwortlich ist, ist die Situation bei einem DSMS differenzierter zu betrachten. So verbleibt auch bei einem installierten DSMS die Verantwortung für die Rechtskonformität bzw. Datenschutzgerechtigkeit eines Verfahrens beim Fachverfahrensverantwortlichen bzw. beim Management einer Organisation. Ein DSB kann nicht dafür verantwortlich gemacht werden, wenn ein Verfahren nicht hinreichend dokumentiert ist oder Daten – entgegen ihrer Zweckbindung – an Dritte weiter gereicht werden. Auch für die Implementation eines DSMS kann ein DSB nicht verantwortlich sein, wohl aber für den Betrieb und dessen permanente Verbesserung. Ein DSB hat die Verantwortung darauf hinzuwirken, dass Indikatoren für Transparenz, Nichtverkettbarkeit und Intervenierbarkeit seitens der Verfahren möglichst automatisiert angeliefert und wiederum automatisiert verarbeitet werden, um seine Planungs- und Kontrollaufgaben technisch auf der Höhe der Zeit durchführen zu können.[8] Die Technik sollte ihn darin unterstützen, dass ein Verfahren nicht in Produktionsbetrieb gehen kann, ohne dass der DSB zuvor die Datenschutzrechtskonformität festgestellt hat.

6 In dieser Publikation von Kersten wird die ISO 27001 im Zusammenspiel mit BSI-Grundschutz vorgestellt, was als Vorlage für die Konzipierung eines DSMS, das die methodische Anlehnung an Grundschutz und PDCA-Zyklus sucht, gut geeignet ist.

7 Diese Privacy-Standards enthalten nur eine Sammlung heterogener Prinzipien sowie Maßnahmen, deren datenschutzrechtliche Anbindbarkeit, im Unterschied zum SDM, im Unklaren bleibt. Deshalb wird das SDM im vorliegenden Ansatz bevorzugt.

3.1 SDM

Das Standard-Datenschutzmodell umreißt einen Rahmen zur Prüfung, Beratung und Auditierung technisch-organisatorischer Schutzmaßnahmen bei personenbezogenen Verfahren (Rost 2012). Es lehnt sich methodisch an das im Informationssicherheitsbereich seit Jahren etablierte Modell zum IT-Grundschutz nach BSI an, ist aber materiellrechtlich an der Umsetzung von Datenschutzanforderungen ausgerichtet, die über Informationssicherheit hinausgehen, ohne dass dies länderspezifisches Datenschutzrecht präjudiziert (vgl. Bock / Meissner 2012). Das Modell orientiert sich am Konzept der Schutzziele (a) sowie an der Nutzung von Schutzbedarfskategorien (b) und betrachtet Verfahren mit Personenbezug differenziert nach Daten, IT-Systemen und Prozessen (c). Hierzu nun:

(a) Mit den sechs elementaren *Schutzzielen* – nämlich Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit – lassen sich die wesentlichen

8 Solche Indikatoren sind, ebenso wie vertrauenswürdige *Prüfanker* in IT-Systemen, erst noch zu entwickeln.

Anforderungen des Datenschutzrechts bzgl. der Zweckbindung, Datensparsamkeit, Erforderlichkeit, Transparenz sowie der Betroffenenrechte in umsetzungsfähige Maßnahmen überführen. Und umgekehrt gestatten sie eine standardisierte Prüfbarkeit von bestehenden Verfahren auf ihre Vereinbarkeit mit dem Datenschutzrecht. Für jedes der sechs Schutzziele gibt es eine Liste mit Maßnahmen, die in unterschiedlichen Graden die Anforderungen eines Schutzziels erfüllen. Ein solcher Katalog mit Maßnahmen enthält für Prüfungen die Referenzmaßnahmen bzw. die Soll-Vorgaben, gegen die die realen Maßnahmen konkreter Verfahren geprüft und beurteilt werden.

(b) Um auf den unterschiedlichen Grad des *Schutzbedarfs* eines personenbezogenen Verfahrens angemessen reagieren zu können, verwendet das Modell drei Schutzbedarfs-Kategorien: normal, hoch und sehr hoch. Die Definitionen des Schutzbedarfs sind, anders als beim IT-Grundschutz, auf die Sicherung der Rechte von Betroffenen ausgerichtet. Die Feststellung des Schutzbedarfs unterliegt einer datenschutzrechtlichen Beurteilung und darf nicht vornehmlich nach rein funktionalen oder wirtschaftlichen Gesichtspunkten erfolgen. Je größer in einer Gesamtschau, die auch Interaktionen und Kontexte berücksichtigt, das Risiko für die Beeinträchtigung der Würde eines Menschen ist, desto höher ist der Schutzbedarf eines Verfahrens. Die Festlegung des Schutzbedarfs muss letztlich der Verfahrensverantwortliche im Rahmen einer Sicherheits- bzw. Risikoanalyse rechtfertigen können.

(c) Bei einem personenbezogenen Verfahren sind drei Komponenten zu unterscheiden und je für sich zu beurteilen und ggfs. zu gestalten. Dies sind: *Daten, IT-Systeme und Prozesse* zur Steuerung der Datenverarbeitung. Diese Differenzierung hat im Wesentlichen den Sinn, Schutz- und Kontrollmaßnahmen so aufeinander abzustimmen, dass sie keine nur punktuelle Wirkung etwa auf der Ebene der Sicherung von IT-Systemen, nicht aber auf der Ebene von Daten haben. Die aus dem Schutzbedarf abzuleitende Schutzwirkung muss für ein Verfahren als Ganzes bestehen.

Bereits anhand dieser knappen Ausführungen zu den drei Komponenten eines SDM zeichnet sich ab, was ein entwickeltes DSMS primär leisten können muss. Es muss standardisiert und verstetigt feststellbar machen,

- welche Verfahren mit Personenbezug eine Organisation nutzt und ob diese Verfahren für die Organisation, für Mitarbeiter und Betroffene sowie für externe Aufsichtsbehörden hinreichend transparent operieren;
- ob und wie die Nichtverkettung von Daten, IT-Systemen und Prozessen im Sinne der Zweckbindung des Verfahrens sowie der Datenverarbeitung gewährleistet ist;
- ob und wie Betroffene ihr Recht durch gesicherten Zugriff auch wirksam durchsetzen können.

Anders formuliert ist von einem DSMS zu fordern, dass es bei Verfahren mit komplexen Systemen und Prozessen sofort und von sich aus Alarm schlägt, weil, allgemein formuliert: Grenzen gegenüber Betroffenen unberechtigt und intransparent überschritten werden die rechtlich gezogen wurden. Dies kann bereits der Fall sein, weil die Prozesse der Dokumentation der IT-Systeme und Prozesse oder die Protokollierung von Abläufen unzureichend ausgelegt sind und damit keine Prüfbarkeit der Beachtung der Grenze möglich ist. Die ISO 27001 legt hierzu vergleichsweise viel Wert auf Dokumentationslenkung.

Alarmieren muss ein DSMS auch in den Fällen, in denen personenbezogene Daten unberechtigterweise dem Einfluss des Betroffenen entzogen oder wenn generell Änderungen an einem Verfahren oder an Infrastrukturen ohne geregeltes Change-Management durchgeführt werden. Beim Change-Management stimmen die Perspektiven von ISMS und DSMS überein: Es dürfen in keinem Falle riskante Änderungen an Verfahren unerkannt, d. h. ohne zurechenbar verantwortete Freigabe vorgenommen werden.

Anschlagen sollte ein DSMS außerdem, wenn Daten anders als durch die Zweckdefinition begrenzt genutzt werden, insbesondere bei Rückgriff auf IT-Systeme. Diese Anforderungen durchzusetzen ist besonders schwierig, weil die Zweckbindung bzw. Nichtverkettbarkeit einer Datenverarbeitung vor allem auf der semantischen Ebene sichergestellt sein muss. Deshalb sind Schulungen für MitarbeiterInnen unerlässlich und sollten von Indikatoren des DSMS erfasst werden. Technisch wirklich sichergestellt werden kann die Zweckbindung im Sinne funktionaler Trennungen erst durch Nutzung von Maßnahmen des Identitätenmanagements.

Die Sicherung der Verfügbarkeit, der Integrität sowie insbesondere der Vertraulichkeit muss selbstverständlich ebenfalls gewährleistet werden. Diesbezügliche Kontrollfunktionen zählen ebenso wie die Absicherung von Daten, die im Rahmen eines DSMS anfallen, zu den Aufgaben eines ISMS. In diesem Beitrag kann es zunächst nur darum gehen, die spezifische Kernfunktionalität eines DSMS zu umreißen.

3.2 ISO 27001

Die ISO 27001 umfasst als Informationssicherheitsmanagementsystem im Wesentlichen drei Komponenten: die vier Phasen des PDCAZyklusses, eine Standardisierung der Unterprozesse dieser vier Phasen des Zyklus' sowie im Annex einen Katalog mit Sicherheitsmaßnahmen.

Als Strategie zur Adaption eines ISMS an ein DSMS liegt dann folgendes Vorgehen nahe: Zu prüfen ist, ob sich für ein DSMS ebenfalls der PDCA-Zyklus als Kernprozessdesign übernehmen lässt und in wie weit die Subprozesse der vier Phasen übernommen werden können oder anzupassen sind. Schlicht zu ersetzen sind dagegen die Schutzmaßnahmen der IT-Sicherheit durch spezifische Datenschutzmaßnahmen, wie sie bspw. als Soll- bzw. Referenzkatalog im Rahmen des SDM in einem ersten Entwurf vorliegen (vgl. Probst 2012).[9]

3.2.1 PDCA

Der PDCA-Zyklus umfasst bekanntlich die folgenden vier Phasen:

- Plan – Planen und Festlegen
- Do – Umsetzen und Betreiben
- Check – Überwachen, Prüfen und Bewerten
- Act – Instandhalten und Verbessern

Der Aspekt der kontinuierlichen Verbesserung betrifft zunächst einmal nur das DSMS selber, noch nicht die (Implementation und stetige Verbesserung von) Verfahren, die mit einem DSMS stetig kontrolliert werden sollen.

Indirekt kann die Übernahme einer solchen Strategie der „nur" kontinuierlichen Verbesserung von Schutzmaßnahmen auf der technisch-organisatorischen Ebene als Eingeständnis begriffen werden, dass Datenschutzrecht technisch-organisatorisch nicht

9 Erste Initiativen für ein Betriebskonzept zur Pflege des Standard-Datenschutzmodells sind seitens des AK-Technik der Datenschutzbeauftragten der Länder und des Bundes auf der DSB-Konferenz im März 2013 gestartet.

so „binär umgesetzt“ ist oder umgesetzt wird, wie es das Datenschutzrecht eigentlich unterstellt nach dem Motto: Betrieb nur dann, wenn eindeutig Rechtskonformität besteht. Der Betrieb eines DSMS auf PDCA-Basis kann insofern bei einem konkreten Verfahren den generellen Verdacht nähren, dass eine Verarbeitung personenbezogener Daten bislang nicht rechtskonform erfolgte, was nun aber nach und nach per DSMS verändert werden soll. Oder es wird festgestellt, dass die Datenverarbeitung von Beginn an rechtlich einwandfrei ist, aber sich der Stand der Technik zur operativen Umsetzung des Rechts weiterentwickelt hat. Ein DSMS wird deshalb die etwaige Unzulänglichkeit bisheriger Datenschutzprüfungen durch DSBe und die strukturelle Überschätzung der Kompetenzen eines DSBen offenbar machen.[10] Ein DSMS auf der Basis des PDCA-Zyklus zu implementieren sollte deshalb pragmatisch mit der Erwartung verbunden sein, dass es vornehmlich darauf ausgerichtet ist, dass sich eine Organisation an permanent wechselnde Umwelten (Änderungen der Gesetzeslagen, organisationsinterne Veränderungen) flexibel, effektiv, sparsam und hinreichend schnell anpassen kann. Bei komplexen Verfahren sind fortgesetzt Maßnahmen zu einem System aufeinander abzustimmen, um eine ganzheitlich systematische Schutzwirkung zu entfalten.[11]

3.2.2 Leitlinie und Definition

Bevor in den Kreisprozess des PDCA-Zyklus eingestiegen wird, verlangt die ISO 27001 zwei Vorbereitungen: Für jedes Managementsystem ist eine Leitlinie unerlässlich. Diese muss formuliert werden, etwa so: Die Organisation verpflichtet sich, sich an die Vorgaben des geltenden Datenschutzrechts zu halten. Und das DSMS verlangt eine Definition, etwa folgender Art:

Ein DSMS ist ein Teil des gesamten Managementsystems. Es benennt die Betroffenen und nimmt je nach Betroffenengruppe gesondert die Risiken in den Blick, die von den Geschäftsprozessen für die Betroffenen bestehen. Auf dieser Grundlage deckt es die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung, Unterstützung und Verbesserung des Datenschutzes der Verfahren der Organisation ab (vgl. Kersten 2011: 41ff).

Ein DSMS ist somit als Teil des gesamten Managementsystems einer Organisation zu begreifen. Ein DSMS fügt sich einerseits in vorhandene Prozessframework wie ISMS, Grundschutz, ITIL usw. ein, hat aber andererseits die Aufgabe, die anderen Aspekte des Managementsystems im Hinblick auf Compliance mit Datenschutzrecht sowie den technischen und organisatorischen Schutzmaßnahmen zu prüfen.

Das DSMS sollte als ein Verfahren verstanden werden, das auf die Risiken für einen Betroffenen durch die Geschäftsprozesse reagiert. Ein DSMS ist insofern ein auf den Einschluss auch organisationsfremder Drittinteressen spezialisiertes System, in dessen Fokus die Umsetzung von Datenschutzanforderungen steht, wie sie bspw. als Schutzziele des Datenschutzes in operationalisierbarer Form formuliert sind.

Das Managementsystem enthält Kriterien, die aus gesetzlichen Regelungen sowie aus weiteren Grundsätzen, Strukturen, Planungsaktivitäten, aus den Verantwortungszuweisungen, best practices, Daten, Prozessen, IT-Systemen und den Ressourcen der Organisation gewonnen werden. Hierfür sind die Begrifflichkeiten festzulegen.

Die Gesamtheit der Aktivitäten, um ein DSMS einzuführen und zu betreiben, ist selbst wiederum als Verfahren zu betrachten, weil es verfahrenseigene Daten erzeugt, IT-Systeme beansprucht und somit Eigentümer eigener Prozesse zur Herstellung der Kontrolle von Datenschutzmaßnahmen ist. Insofern muss das DSMS seinerseits datenschutzgerecht eingerichtet und betrieben werden.

3.2.3 PLAN

(a) Zu planen und zu entscheiden sind in Bezug zu einem DSMS die folgenden Aspekte:
- Welche Ziele verfolgt die Organisation mit dem Betreiben eines DSMS?
- Welchen Datenschutz-Anforderungen hat eine Organisation zu genügen?
- Welche Anforderungen stellt die Organisation an ein funktionierendes DSMS?
- Welchen Anwendungsbereich soll das DSMS anfänglich umfassen?
- Welcher Geschäftsplan oder welche Rechtsgrundlage liegt der DSMS-Einführung zugrunde?

Die Beantwortung dieser Fragen sollte in einer Entscheidungsvorlage verdichtet werden. Diese Vorlage sollte u. a. insbesondere auf die gesetzlichen Anforderungen eingehen, die Beschreibung der Rolle des Datenschutzbeauftragten sowie einen Geschäfts- und Zeitplan zur Umsetzung beinhalten.

Beim Umreißen der Aufgaben eines DSMS wären dann die folgenden Punkte anzusprechen:
- Die Datenschutzmaßnahmen, die ein DSMS entsprechend der vom SDM nahegelegten Methodik bereitstellt.
- Die Sichtbarkeit des Stands bzgl. des Datenschutzes und dessen Aufrechterhaltung (Stichwort: Reifegradmodell, „CMMI“, ISO 9001).

(b) Es muss der Anwendungsbereich des DSMS festgelegt werden, typischerweise sind sämtliche Aktivitäten einer Organisation betroffen. Es sind auch die Grenzen auszuweisen, hier insbesondere zum ISMS, um Verantwortlichkeiten eindeutig festlegen zu können.

(c) Die Methode der Risikoeinschätzungen ist festzulegen. Diese sollte sich des SDM bzw. der sechs elementaren Schutzziele bedienen. Festzulegen ist, wie mit verbleibenden Risiken umgegangen wird. Während in einem ISMS Risiken relativ leicht akzeptiert werden können, indem sie „einfach verantwortet“ und bezifferbar versichert werden können, kann dies bei Interessen Dritter ganz anders sein. Hier müssen wesentliche Risiken für Betroffene in einem DSMS tatsächlich bearbeitet und Maßnahmen der *breach response*, also des Umgangs mit Datenschutz-Vorfällen festgelegt werden. Wenn sich keine Lösung abzeichnet oder eine Fachaufsicht, ein neuer Partner, die Unternehmenshaftpflichtversicherung oder eine Aufsichtsbehörde negativ intervenieren, dann muss ein DSMS Wirkungen eines *show stoppers* entfalten können, indem bspw. datenschutzriskante Geschäftsprozesse beendet oder gar nicht erst aufgesetzt werden (können). Typisch wäre jedoch, zur Risi-

10 Dieser Gedanke betrifft die absehbaren Widerstände gegen die Einführung solcher Systeme.

11 In der Hinwendung zu Risiko basierten, kontinuierlich-iterativen Verbesserungsprozessen drückt sich in der Datenschutzpraxis die Umstellung von Modellierungen in kausalen Ablaufketten-auf Korrelationen von Ereignissen aus (vgl. dazu Pohle 2013).

kobehandlung die Entwicklung von Schutzmaßnahmen, einschließlich der Indikatoren zur Messung der Wirksamkeit, als Projekt aufzusetzen.
(d) Es sind Fortbildungsmaßnahmen in Bezug auf Datenschutzrecht zu planen.

3.2.4 DO

Um ein DSMS ans Laufen zu bringen und es am Laufen zu halten, sind die folgenden Anforderungen umzusetzen:
(a) Es sind Risikobehandlungsaktivitäten zu entfalten. Dazu zählen die folgenden Aspekte:
- Die DSMS-Leitlinie ist in Kraft zu setzen.
- Die Bedeutung der Leitlinie ist zu vermitteln.
- Es sind Maßnahmen der Risikoeinschätzung und deren Behandlung einzurichten.
- Es sind Verantwortlichkeiten festzulegen.
- Es sind Ressourcen für alle Phasen eines DSMS bereit zu stellen.
- Es sind Ausbildung-, Fortbildungs sowie Sensibilisierungsmaßnahmen für Mitarbeiter vorzunehmen.
- Es sind *breach response*-Fälle zu bearbeiten.
- Es sind DSMS-Audits sowie Managementbewertungen des DSMS durchzuführen.

(b) Die Umsetzen des Risikobehandlungsplans ist unter Datenschutzaspekten problematisch. Der Plan muss Strategien enthalten, aus denen hervorgeht, wie eine derzeit nicht-rechtskonforme Situation in eine rechtskonforme Situation überführt wird und wie in der Zwischenzeit mit dem nicht-rechtskonformen Zustand umgegangen wird.
(c) Es sind die auf der Grundlage des SDM abgeleiteten Schutzmaßnahmen umzusetzen. Kommen andere Schutzmaßnahmen als die vom Modell präferierten zum Einsatz, so muss deren funktionale Äquivalenz belegt werden.
(d) Es sind die Indikatoren zur Abschätzung der Wirksamkeit der Maßnahmen zu entwickeln und einzusetzen.
(e) Unverzichtbar ist eine Sensibilisierung der Mitarbeiter.
(f) Der Betrieb des DSMS ist seinerseits zu verwalten. Das bedeutet bspw. dass ein DSMS etwa mit den standardisierten Methoden nach ITIL, über ein Ticketsystem *incidents*, *problems* und *changes* in Bezug auch auf die DSMS-eigenen Strukturen, zur Alarmierung der zu kontrollierenden Verfahren verwaltet.
(g) Insofern bedarf es eines eigenen Ressourcenmanagements für das DSMS.

3.4.5 CHECK

(a) Es ist eine Überwachung und regelmäßige Überprüfung der Compliance mit Datenschutzrecht sowohl des DSMS selbst als auch der zu kontrollierenden Verfahren einzurichten.
(b) Es muss eine Abschätzung der Wirksamkeit der Schutzmaßnahmen und deren Überprüfbarkeit vorgenommen werden.
(c) Die Risikoeinschätzungen sind regelmäßig zu wiederholen.
(d) Audits des DSMS sind durchzuführen.[12]
(e) Ein DSMS ist seitens des Managements zu bewerten.
(f) Die Ressourcenplanung, Schulungen, Audits, Datenschutzvorfälle, Abschätzung der Wirksamkeit der Maßnahmen, Managementbewertungen sind zu dokumentieren.

3.2.6 ACT

(a) Identifizierte Verbesserung sind umzusetzen.
(b) Korrekturen, Vorbeugemaßnahmen und
(c) Kommunikation der beabsichtigen Verbesserungen sind vorzunehmen.
(d) Auch hier muss eine Erfolgskontrolle der Verbesserungen seitens des Managements vorgenommen werden.

4 Fazit

Wenn man das SDM, den PDCA-Zyklus und die standardisierten Subprozesse der ISO 27001 miteinander kombiniert, zeichnen sich die Umrisse eines DSMS ab, die den hochgesteckten Anforderungen bezüglich der stetigen Überprüfbarkeit von komplexen personenbezogenen Verfahren, einschließlich ihres laufenden Wandels, genügen könnten. Es zeigt sich aber auch, dass schon in Bezug auf die Standardisierung von Datenschutzmaßnahmen und Datenschutzprüfungen, wie sie auf der Grundlage des SDM vorgeschlagen wird, noch sehr viel zu tun bleibt.

Literatur

Bock / Meissner, 2012: Datenschutz-Schutzziele im Recht – Zum normativen Gehalt der Datenschutz-Schutzziele; in: DuD 2012/06: 425-431.

BSI-ISOGS, o.J.: ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz (verfügbar im Internet)

CBP 2013: Richtsnoeren beveiliging van persoonsgegevens, http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf, English-Summary: http://www.newsletternautadutilh.com/ downloads/Privacy/summary_ guidelines_ENG.PDF.

Hansen, Marit / Pfitzmann, Andreas, 2010: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetec-tability, Unobservability, Pseudony-mity, and Identity Management, (v0.34) (verfügbar im Internet).

ISO 27001, o.J.: Beuth-Verlag, http://www.beuth.de/.

Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner, 2011: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Der Weg zur Zertifizierung, 3. Auflage, Viewg+Teubner Verlag / Springer Fachmedien Wiesbaden.

Kongehl, Gerhard (Hrsg.), 2006: Datenschutzmanagement, WRS-Verlag.

Looman / Matz 2010: Datenschutzmanagement-Standard (verfügbar im Internet)

Meints, Martin, 2006: Datenschutz nach BSI-Grundschutz? in: DuD 2006/10: 13-16.

Meints, Martin, 2007: Datenschutz durch Prozesse; in: DuD 2007/02: 91-95.

Pohle, Jörg, 2013: Kausalitäten, Korrelationen und Datenschutzrecht. Beitrag zum Workshop „Fundationes I: Geschichte und Theorie des Datenschutzes", im Erscheinen. http://waste.informatik.hu-berlin.de/~pohle/papers/korrelationen_20130203.pdf.

Prietz, Christian, 2012: Musterprozesse zum Datenschutzmanagement, in: DuD 2012/01: 14-19.

Probst, Thomas, 2012: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD 2012/06: 439-444.

Quiring-Kock, Gisela, 2012: Anforderungen an ein Datenschutzmanagementsystem – Aufbau und Zertifizierung; in: DuD 2012/11: 832-836.

Rost, Martin, 2012: Standardisierte Datenschutzmodellierung; in: DuD 2012/06: 433-438.

Rost, Martin, 2013: Eine kleine Geschichte des Prüfens, Beitrag für den BSI-Sicherheitskongress 2013 (Konferenzband ist im Erscheinen).

ULD, 2002: Informationen für die schleswig-holsteinische Wirtschaft: Betriebliches Datenschutzmanagement nach dem BDSG (verfügbar im Internet).

12 Für Zertifizierungen von DSMS stehen beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein mit dem Datenschutz-Gütesiegel und dem EuroPriSe-Siegel bereits reife Verfahren zur Verfügung.