SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 04-12-019

ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in das ITIL-Framework

Michael Klotz
Jörn Kriegel

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

August 2012

ISSN 1868-064X

Klotz, Michael; Kriegel, Jörn, Vorname: ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in das ITIL-Framework. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2012 (SIMAT AP, 4 (2012), 19), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat04120199

Impressum
Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber
Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autor
Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten Unternehmensorganisation und Informationsmanagement. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., wissenschaftlicher Beirat und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

Jörn Kriegel ist seit 2001 Beauftragter für Datenschutz und Datensicherheit bei der IKB Deutsche Industriebank AG. Er studierte an den Universitäten in Erlangen, Krakau und London.

Die „SIMAT Arbeitspapiere“ dienen einer möglichst schnellen Verbreitung von Forschungs- und Projektergebnissen des SIMAT. Die Beiträge liegen jedoch in der alleinigen Verantwortung der Autoren und stellen nicht notwendigerweise die Meinung der FH Stralsund bzw. des SIMAT dar.

ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL

Prof. Dr. Michael Klotz, Jörn Kriegel[1]

Zusammenfassung: Die „IT Infrastructure Library“ (ITIL) gilt heute als weltweit führender De-facto-Standard für das IT-Servicemanagement (ITSM). Obwohl der Standard mittlerweile in der in 2007 veröffentlichten dritten Version vorliegt, haben Datenschutzbelange bis heute kaum Eingang gefunden. Das Arbeitspapier zeigt auf, wie und wo Datenschutz in ITIL einbezogen werden kann und muss. Diese Diskussion wird anhand der in ITIL beschriebenen IT-Prozesse geführt. Es wird exemplarisch gezeigt, dass aus einer detaillierten Analyse eines ITIL-Prozesses – hier das Lieferantenmanagement (Supplier Management) – verschiedene Ansatzpunkte für eine Integration des Datenschutzes in ein IT-Servicemanagement nach ITIL resultieren. Diskutiert werden die Nutzung eines eigenen Datenschutzservice, die Einbeziehung des Datenschutzes als Servicebestandteil, die Prozessintegration des Datenschutzes und der Datenschutz als Ausprägung von Prozesselementen. Hieraus ergibt sich letztlich die Rolle des betrieblichen Datenschutzbeauftragten (DSB) als Stakeholder in den IT-Prozessen nach ITIL. Diese kann durch insgesamt sechs Beteiligungsformen ausgefüllt werden: Dem DSB kann für einzelne Aufgaben eines IT-Prozesses nach ITIL eine Verantwortung für die Prozessdurchführung und/oder das Prozessergebnis obliegen. Er kann als Initiator des Prozesses insgesamt oder einzelner Aufgaben in der Prozesskette fungieren. Im Rahmen der Prozessdurchführung hat er mitunter Stellungnahmen zu datenschutzrelevanten Fragen zu erarbeiten und er kann Mitglied von Gremien und Arbeitsgruppen sein. Hinsichtlich des Informationsmanagements ist er definierter Empfänger prozessualer Informationen und Adressat von Berichten. Um diese verschiedenen Funktionen ausführen zu können, ist er zudem Nutzer von ITSM-Tools. In der Summe all dieser Beteiligungsmöglichkeiten und letztlich auch Beteiligungsnotwendigkeiten steht die Schlussfolgerung, dass der DSB an der Durchführung und Verbesserung der ITIL-spezifischen IT-Prozesse grundsätzlich mitzuwirken hat. Wie umfangreich diese Mitwirkung und seine diesbezügliche Verantwortlichkeit ausfällt, erfordert eine Analyse im Einzelfall, die sich auf die unternehmensspezifische Intensität der Beziehungen

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de; Jörn Kriegel, Beauftragter für Datenschutz und Datensicherheit der IKB Deutsche Industriebank AG, Wilhelm-Bötzkes-Str. 1, 40474 Düsseldorf, Joern.Kriegel@ikb.de

zwischen dem Datenschutz und der jeweiligen Ausprägung des IT-Servicemanagements nach ITIL richtet.

Gliederung

Vorwort des Herausgebers 5
Abkürzungsverzeichnis 6
Abbildungsverzeichnis 8
Tabellenverzeichnis 9
1 Einleitung 10
2 ITIL und Datenschutz – Notwendiger Zusammenhang 12
2.1 Informationssicherheit 13
2.2 Auftragsdatenverarbeitung 16
2.3 Zusammenfassung der gegenseitigen Bezüge 19
3 Ansatzpunkte für eine Integration des Datenschutzes in ITIL 20
3.1 Datenschutzgesetzliche Anforderungen in den ITIL-Prozessen 22
3.2 Datenschutz als Service 24
3.3 Datenschutz als Servicebestandteil 26
3.4 Prozessintegration des Datenschutzes 28
3.4.1 Prozessintegration als Aufgabeninhalt 29
3.4.2 Prozessintegration als Prozessanforderung 30
3.4.3 Prozessintegration im Rahmen der Nutzung von Tools 34
3.5 Einbindung des Datenschutzbeauftragten als Stakeholder 34
4 Unternehmensindividuelle Analyse und Umsetzung 38
Literaturangaben 42

Schlüsselwörter: Auftragsdatenverarbeitung – Datenschutz – Datenschutzbeauftragter – BDSG – ITIL – IT-Prozess – IT-Service – IT-Servicemanagement – Informationssicherheit – Informationssicherheitsmanagement – Lieferantenmanagement

JEL-Klassifikation: L15, L24, M21

Hinweis: Aus Gründen der besseren Lesbarkeit wird in der Regel die männliche Schreibweise verwendet. Es sei an dieser Stelle ausdrücklich darauf hingewiesen, dass sowohl die männliche als auch die weibliche Schreibweise gemeint ist.

Vorwort des Herausgebers

Datenschutz und ITIL: Auf den ersten Blick ist dies eine ungewöhnliche Verbindung – aber keine unsinnige, wie dieses Arbeitspapier zeigen soll. Der Blickwinkel ist derjenige des Datenschutzes, also einer Aufgabe, die zwar gesetzlich verankert ist, aber trotzdem nicht immer die notwendige Aufmerksamkeit in Unternehmen und sonstigen Organisationen erfährt. Eine Lösung eröffnet die Integration des Datenschutzes in die IT-Prozesse. Wie diese Integration aussehen kann (und soll), wird anhand des führenden Standards des IT-Servicemanagements, der „Information Technology Infrastructure Library“ (ITIL) diskutiert. Über den Grad der Integration lässt sich streiten, über die grundsätzliche Notwendigkeit nicht – so die Überzeugung der Autoren. Wo der Datenschutz in die IT-Prozesse nach ITIL integriert ist, winken Compliance und Effizienzgewinne.

Mit dem vorliegenden Arbeitspapier kann jedes Unternehmen basierend auf den hier angestellten Überlegungen seine individuelle Beziehung zwischen ITIL und Datenschutz reflektieren. In diesem Sinne wünsche ich eine gewinnbringende Lektüre.

Prof. Dr. Michael Klotz

Diese Arbeit wurde unterstützt von den Unternehmen

IKB AG, Düsseldorf

Serview GmbH, Bad Homburg

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCTA	Central Computer and Telecommunications Agency
CI	Configuration Item
CMS	Configuration Management System
CO	Cabinet Office
DS	Datenschutz
DSB	Datenschutzbeauftragter
DV	Datenverarbeitung
FTP	File Transfer Protocol
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISO	International Organization for Standardization
ISP	Information Security Policy
IT	Information Technology, Informationstechnik
ITGI	IT Governance Institute
ITSM	IT-Servicemanagement
itSMF	IT Service Management Forum
ITIL	Information Technology Infrastructure Library
KEDB	Know Error Database
OGC	Office of Government Commerce
OLA	Operational Level Agreement
PIN	Personal Identification Number
pD	personenbezogene Daten
RFC	Request for Change
SACM	Service Asset and Configuration Management
SCA	Service Capability Asset
SCD	Supplier and Contract Database
SD	Service Design
SIP	Supplier Service Improvement Plan
SLA	Service Level Agreement
SLP	Service Level Package
SLM	Service Level Management
SLR	Service Level Requirement
SO	Service Operation

SS	Service Strategy
ST	Service Transition
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
V3	Version 3
VBF	Vital Business Function
VPN	Virtual Private Network

Abbildungsverzeichnis

Abb. 1	BDSG-Paragrafen zur Informationssicherheit	14
Abb. 2	BDSG-Paragrafen zur Auftragsdatenverarbeitung und Informationssicherheit	17
Abb. 3	Zusammenhänge zwischen Auftragsdatenverarbeitung und Supplier Management	18
Abb. 4	Ausgewählte Zusammenhänge zwischen BDSG und ITIL	19
Abb. 5	Ansatzpunkte für eine Integration des Datenschutzes in ITIL	21
Abb. 6	Datenschutz-SLP als Kombination verschiedener Servicekomponenten	27
Abb. 7	Prozessuale Integration des Datenschutzes	28
Abb. 8	Der DSB als Stakeholder	35
Abb. 9	Vorgehen zur Integration des Datenschutzes in ITIL	39

Tabellenverzeichnis

Tab. 1 Informationssicherheitsmaßnahmen nach BDSG 15
Tab. 2 Verweise auf gesetzliche und regulatorische Anforderungen in ITIL-Prozessen 22
Tab. 3 Verweise auf datenschutzrechtliche Anforderungen in ITILProzessen 23
Tab. 4 IT-Prozesse mit wesentlichen datenschutzrelevanten Handlungsobjekten 31
Tab. 5 IT-Prozesse und ITSM-Tools 34
Tab. 6 Stakeholder-Matrix für die Prozessintegration des DSB 38
Tab. 7 Bewertung der DS-Integration in die ITIL-Prozesse 40
Tab. 8 Maßnahmen für den Prozess „Supplier Management“ 41

1. Einleitung

ITIL als Standard für das ITSM

Die „IT Infrastructure Library“ (ITIL[2]) gilt heute als weltweit führender De-facto-Standard für das IT-Servicemanagement (ITSM).[3] Durch ein professionelles IT-Servicemanagement soll sichergestellt werden, „dass die IT-Infrastruktur und die in ihr integrierten Anwendungssysteme, Prozesse und Mitarbeiter bestmöglich aufeinander abgestimmt sind und geschäftliche Anforderungen unterstützen“.[4] Gemeinsam mit der Norm ISO/IEC 20000 wird ITIL[5] von Unternehmen als meistgenutzter Standard genannt, um diese Zielsetzung zu erreichen.[6] Diejenigen Unternehmen, die sich explizit mit IT-Servicemanagement auseinandersetzen, richten ihr ITSM fast durchgängig an ITIL aus.[7]

Zertifizierung

Während sich in Bezug auf ITIL nur Personen zertifizieren lassen können[8], ist eine institutionelle Zertifizierung des IT-Servicemanagements einer IT-Organisation nach der Norm ISO/IEC 20000 möglich.[9] Viele Unternehmen nutzen das ITIL-Rahmenwerk jedoch auch ohne formelle Zertifizierung als Grundlage eines eigenen Hausstandards zum IT-Servicemanagement.

Library

ITIL war ursprünglich lediglich eine Reihe von Büchern, in denen Best-Practice-Wissen als Leitfaden für das Management von IT-Services dokumentiert wurde. Auf diesen Status geht dann auch die Bezeichnung „Library“ zurück. Heute besteht ITIL neben den nach wie vor so bezeichneten, nunmehr fünf Büchern[10] aus allen Ingredienzien, die eine erfolgreiche Ver-

---

[2] ITIL® is a Registered Trade Mark of the Cabinet Office in the United Kingdom and other countries.
[3] Vgl. *Zarnekow/Brenner 2004*, S. 7; *BSI 2005*, S. 6; *Johannsen/Goeken 2011*, S. 196.
[4] *Johannsen/Goeken 2011*, S. 201.
[5] In Anlehnung an den überwiegenden Sprachgebrauch wird im Folgenden auf die Verwendung des Artikels („die ITIL“) verzichtet.
[6] Vgl. *ITGI 2011*, S. 29; in der weltweiten Umfrage zum Status der Umsetzung von IT-Governance in Unternehmen haben 28 % der Befragungsteilnehmer geantwortet, dass sie ITIL/ISO 20000 als Grundlage ihrer IT-Governance verwenden.
[7] Vgl. *Materna 2010*, 15; in der Umfrage gaben 94 % der Befragungsteilnehmer an, dass sie auf die Nutzung der ITIL setzen. Über 90 % derjenigen Befragten, die ITIL einsetzen, empfehlen die Nutzung der ITIL.
[8] Die persönliche ITIL-Kompetenz kann in verschiedenen Zertifizierungsstufen nachgewiesen werden. Den Einstieg stellt das „ITIL Foundation Certificate“ dar.
[9] Die ISO/IEC 20000 besteht aus fünf Teilen, wobei bei der Zertifizierung die Einhaltung der Vorgaben aus der ISO/IEC 20000 Part 1 – „Service Management System Requirements" geprüft wird. Für einen Überblick zur Vorbereitung und zum Ablauf der Zertifizierung siehe *Dohle u. a. 2009*, S. 10-14, sowie die dortige Darstellung der Fallstudien, S. 107-152.
[10] Diese sind: Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement.

breitung und Vermarktung eines Management-Konzeptes ausmachen: Trainingsangebote bis hin zu qualifizierenden Zertifikatsabschlüssen, professionelle Beratung und unabhängiger Erfahrungsaustausch innerhalb spezieller Organisationen,[11] Umsetzungshilfen und Software-Tools.

ITIL-Urheber

Ursprünglich wurde ITIL in den Jahren von 1989 bis 1994 federführend durch die Central Computer and Telecommunications Agency (CCTA), einer IT-Dienstleistungsorganisation der britischen Regierung, unter umfangreicher Beteiligung von IT-Experten und -Praktikern entwickelt.[12] Heute liegen die Rechte an ITIL beim Cabinet Office (CO)[13], das sie im Zuge einer Umstrukturierung der britischen Verwaltung vom Office of Government Commerce (OGC) übernommen hat. Die Erarbeitung von ITIL erfolgte in Zusammenarbeit mit Experten, Beratern und erfahrenen Berufspraktikern. Mit der Zeit wurde ITIL eine umfassende, nicht-proprietäre, öffentlich publizierte und damit allgemein zugängliche Verfahrensempfehlung für die Planung, Überwachung und Steuerung von anspruchsvollen IT-Dienstleistungen. Heute ist ITIL in Unternehmen weltweit verbreitet und es gibt eine große Anzahl an IT-Professionals, die zur weiteren Verbreitung und Implementierung von ITIL in Unternehmen und öffentlichen Verwaltungen beitragen.

ITIL und Datenschutz

Trotz dieser beachtlichen Entwicklung finden Datenschutzbelange bis heute, d. h. auch in der aktuellen, im Mai 2007 veröffentlichten dritten Version (abgekürzt „ITIL V3“) kaum Berücksichtigung. Allerdings liegt diese Verbindung offensichtlich auch nicht auf Hand – zumindest wird sie in der Fachwelt kaum thematisiert.[14] Wenn im Folgenden der Zusammenhang von ITIL und Datenschutz (DS) diskutiert werden soll, muss somit zuerst die Sinnhaftigkeit dieses Unterfangens begründet werden. Hierfür wird es als ausreichend erachtet, die Notwendigkeit des Zusammenhangs an zwei

---

[11] Das „IT Service Management Forum“ (itSMF) ist eine weltweit tätige, unabhängige Organisation, die den Erfahrungsaustausch der ITSM-Experten organisiert. In Deutschland nimmt der 2001 gegründete itSMF Deutschland e.V. die Vernetzungsfunktion wahr, vgl. http://www.itsmf.de/.

[12] Vgl. *Köhler 2006*, S. 24; *Huber 2009*, S. 16.

[13] Das Cabinet Office entspricht in seiner Stellung und Funktion in etwa dem deutschen Kanzleramt.

[14] Die Google-Abfrage mit den beiden Suchtermen „Datenschutz und ITIL“ sowie „ITIL und Datenschutz“ ergab lediglich 5 bzw. 4 Treffer (Abfrage am 21.07.2012). Auch die Ausführungen der BSI-Broschüre „ITIL und Informationssicherheit“ (*BSI 2005*) enthalten keinerlei Bezüge zum Datenschutz. Ebenso führen die verschiedenen ITIL- und ITSM-Publikationen den Begriff „Datenschutz“ nicht in ihrem Index auf, s. bspw. *Bock 2010*, *Böttcher 2010*, *Dohle u. a. 2009*, *Huber 2009*.

exemplarischen Beispielen darzustellen. Weitere Zusammenhänge werden im Verlauf der Arbeit aufgezeigt. Auf dieser Basis soll die Untersuchung sodann in zwei Richtungen vorgenommen werden:

- Zum einen soll analysiert werden, wie und wo Datenschutz in ITIL einbezogen werden kann oder auch muss. Hierzu werden die ITIL-Prozesse der vier Domänen Service Strategy, Service Design, Service Transition und Service Operation betrachtet. Eine detaillierte Analyse zeigt die verschiedenen Möglichkeiten und Notwendigkeiten der Berücksichtigung des Datenschutzes in den IT-Prozessen nach ITIL auf.
- Zum anderen stellt sich die Frage, wo in den verschiedenen Prozessen der betriebliche Datenschutzbeauftragte (DSB) zu verorten ist. Diese Diskussion wird anhand der in ITIL beschriebenen IT-Prozesse, d. h. exemplarisch für das Lieferantenmanagement (Supplier Management), geführt. Aus der Antwort ergibt sich letztlich die Rolle des betrieblichen Datenschutzbeauftragten (DSB) als Stakeholder in den IT-Prozessen nach ITIL.

Zielsetzung

Ziel der Darstellung ist es, den Datenschutz in den IT-Prozessen nach ITIL zu verankern. Praktisch führt dies zu einer Integration des Datenschutzes in den jeweiligen ITIL-Hausstandard, der vom fachlichen Know-how der für den Datenschutz Verantwortlichen profitieren kann. Umgekehrt erfährt der Datenschutz durch diese operative Integration eine erhöhte Aufmerksamkeit und stärkere Durchdringung im Unternehmen. Dies dürfte sich auch positiv auf die Stellung des betrieblichen Datenschutzbeauftragten auswirken. Durch eine operative Integration in die ITIL-Prozesse erhält der DSB die Chance, sich vom Rand des ITIL-Geschehens zu lösen und als Beteiligter („Stakeholder“) auf Augenhöhe an der datenschutzbezogenen Gestaltung, Durchführung und Verbesserung der ITIL-spezifischen IT-Prozesse mitzuwirken.

2. ITIL und Datenschutz – Notwendiger Zusammenhang

BDSG als Ausgangspunkt

Datenschutz kann aus unterschiedlichen Perspektiven betrachtet werden. Aus Unternehmenssicht stellen Mitarbeiter- und Kundendaten einen immateriellen Vermögensgegenstand dar, den es zu schützen gilt. Für die Betroffenen stehen der Schutz der Privatsphäre und die Sicherstellung ihres informationellen Selbstbestimmungsrechts im Vordergrund. Die hier vorgenommene unternehmensbezogene Diskussion eines Zusammenhangs zwi-

schen ITIL und Datenschutz soll für den Datenschutz aus Sicht des Bundesdatenschutzgesetzes (BDSG) vorgenommen werden, also einer Rechtsnorm, die von Unternehmen im Geschäftsalltag zu befolgen ist. Dem liegt folgende Überlegung zugrunde: Wenn die in ITIL beschriebenen IT-Prozesse Vorgaben aus dem BDSG zu berücksichtigen haben, resultiert hieraus eine unabweisbare Notwendigkeit der Einbeziehung des Datenschutzes in ITIL – weil gesetzliche Vorgaben nun einmal innerhalb der IT-Prozesse zu befolgen sind. Ebenso resultiert hieraus die Notwendigkeit der Einbeziehung des Datenschutzbeauftragten, weil dieser im Unternehmen nach § 4g Abs. 1 Satz 1 BDSG auf die Einhaltung datenschutzgesetzlicher Vorschriften hinzuwirken hat.[15]

Aus dem BDSG ergeben sich zwei offensichtliche Bereiche, die mit dem IT-Servicemanagement in Zusammenhang stehen. Dies sind zum einen Maßnahmen der Informationssicherheit, zum anderen die in der BDSG-Novelle vom Juni 2009 ergänzten Regelungen zur Auftragsdatenverarbeitung.

2.1 Informationssicherheit

Sicherheit personenbezogener Daten

Das BDSG schreibt nicht nur den Schutz, sondern auch die Sicherheit personenbezogener Daten (pD) vor.[16] Die betreffenden Regelungen finden sich in den §§ 4e, 4g und 9 BDSG sowie der Anlage zu § 9 BDSG. Die Verweisungsstruktur ist in Abbildung 1 dargestellt.

Nach § 4g Abs. 2 Satz 1 BDSG ist vom Unternehmen eine Übersicht (sog. Verfahrensübersicht oder -verzeichnis) zu erstellen, die die in § 4e Satz 1 BDSG aufgeführten Angaben enthalten soll. Nach § 4e Satz 1 Nr. 9 BDSG hat sich diese Darstellung auch auf die zur Gewährleistung der „Sicherheit der Verarbeitung“ ergriffenen Maßnahmen gemäß § 9 BDSG zu richten. Die Beschreibung hat so detailliert zu erfolgen, dass eine Beurteilung der Angemessenheit möglich ist; sie geht damit über eine allgemeine, grobe Darstellung deutlich hinaus.

---

[15] Diese Begründung rekurriert letztlich auf die Sicherstellung von IT-Compliance in Form der Einhaltung gesetzlicher Vorgaben, hier aus dem BDSG und weiteren Gesetzen, die sich auf den Datenschutz richten, z. B. dem Telekommunikationsgesetz (TKG) oder dem Telemediengesetz (TMG), vgl. *Klotz 2011*.

[16] Vgl. *Witt 2008*, S. 121, der darauf hinweist, dass Datenschutz und IT-Sicherheit zwar unterschiedliche Ziele verfolgen, die jeweiligen Maßnahmen – wenn auch nicht deckungsgleich – jedoch meist vergleichbar sind. Auf der begrifflichen Seite soll im Folgenden jedoch von Informationssicherheit gesprochen werden, da sich das BDSG in § 32 Abs. 2 auf personenbezogene Daten in jedweder Form bezieht, d. h. auch auf Daten in Papierdokumenten, wie z. B. der Personalakte.

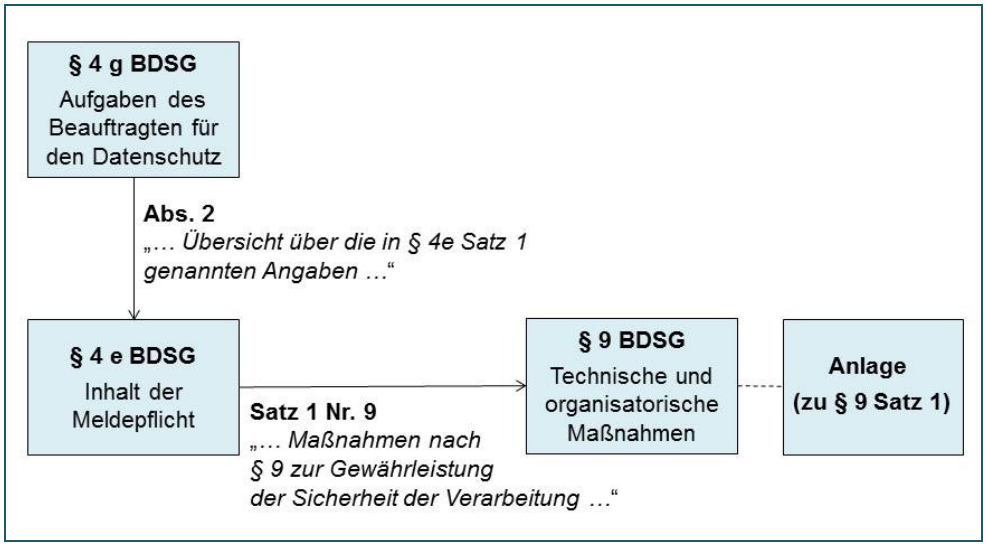

Abbildung 1
BDSG-Paragrafen zur Informationssicherheit

Anlage zu § 9 Satz 1 BDSG

Die zu treffenden Vorkehrungen werden in § 9 BDSG als technische und organisatorische Maßnahmen konkretisiert. Die Anlage zu § 9 Satz 1 BDSG benennt als solche sieben Kontrollpflichten und ein Zwecktrennungsgebot in Bezug auf die Verarbeitung personenbezogener Daten, die insgesamt den Schutz personenbezogener Daten sicherstellen sollen. Tabelle 1 listet diese Vorgaben im Einzelnen auf. Die genannten Maßnahmen entsprechen durchgängig allgemein üblichen Maßnahmen der Informationssicherheit. Insofern erweisen sich die hier genannten Schutzvorkehrungen in Bezug auf personenbezogene Daten als Untermenge des State-of-the-Art eines Informationssicherheitsmanagements.

Informationssicherheit in ITIL

Innerhalb von ITIL ist der IT-Prozess „Information Security Management“ (ISM) Teil des Buches „Service Design“.[17] Allein schon die Tatsache, dass das BDSG die Informationssicherheit im oben beschriebenen Umfang adressiert, spricht prima facie dafür, dass der ISM-Prozess nach ITIL Datenschutzbelange zu berücksichtigen hat und dass ebenso der Datenschutzbeauftragte am ISM-Prozess umfänglich beteiligt sein muss.

Privacy in ITIL

In den Ausführungen zum Information Security Management findet sich eine der wenigen Stellen in ITIL, in der explizit auf Datenschutz eingegangen wird. Hier wird die Notwendigkeit der Umsetzung regulatorischer Vorgaben in Bezug auf Datenschutz mit Hilfe spezieller Technologien („privacy compliance technologies“) betont.[18] Diese und weitere gelegentliche Erwäh-

[17] Siehe *ITIL SD 2007*, S. 141-149.
[18] Siehe *ebd.*, S. 145; vgl. Tabelle 2 in Abschnitt 3.1.

nungen des Datenschutzes lassen vermuten, dass ITIL Datenschutz zwar als integralen Teil des ISM betrachtet, ihn jedoch nicht als eigenständiges Thema einstuft.

Tabelle 1
Informationssicherheitsmaßnahmen nach BDSG[19]

Nr.	Vorgabe	Maßnahmen
1	Zutrittskontrolle	• Verwehren des Zutritts von Unbefugten zu DV-Anlagen, mit denen pD verarbeitet oder genutzt werden
2	Zugangskontrolle	• Verhindern, dass DV-Systeme von Unbefugten genutzt werden können
3	Zugriffskontrolle	• Zugriff auf Daten durch Berechtigte ausschließlich gemäß ihrer Zugriffsberechtigung • Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen von pD bei Verarbeitung/Nutzung, nach Speicherung
4	Weitergabekontrolle	• Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen von pD bei Übertragung/Transport oder Speicherung • Prüfung und Feststellung, an welchen Stellen eine Übertragung von pD vorgesehen ist
5	Eingabekontrolle	• Prüfung und Feststellung, ob/von wem pD in DV-Systeme eingegeben, verändert oder entfernt worden sind
6	Auftragskontrolle	• Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers
7	Verfügbarkeitskontrolle	• Schutz von pD vor Zerstörung oder Verlust
8	Zwecktrennungsgebot	• Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten

Bezüge BDSG/ISM-Prozess

Neben diesem ausdrücklichen Bezug auf den Datenschutz finden sich in den Ausführungen zum ISM-Prozess Überschneidungen zum BDSG dort, wo Sicherheitskontrollen angesprochen werden. So sind nach ITIL im Rahmen des ISM-Prozesses Sicherheitskontrollen zu implementieren, die sich auf den Zugang zu Services, Systemen und Informationen richten.[20] Grundlage hierfür ist eine Informationssicherheitsrichtlinie, die Vorgaben z. B. für Zugriffs- oder Passwort-Kontrollen enthalten soll. Dies entspricht teilweise wortwörtlich den in der Anlage zu § 9 Satz 1 BDSG genannten Kontrollen. Ebenso sollen nach ITIL in der Informationssicherheitsrichtlinie Vorgaben zur Klassifizierung von Informationen und Dokumenten enthalten sein. Eine Datenklassifizierung ist jedoch wiederum als Voraussetzung anzusehen, um personenbezogene Daten bei der Definition von Sicherheitsstufen ange-

[19] Verkürzt wiedergegeben nach § 9 Satz 1 BDSG.
[20] Siehe *ITIL SD 2007*, S. 141.

messen zu berücksichtigen und damit die Vorgaben des BDSG umzusetzen.[21]

Im ISM-Prozess finden sich zahlreiche weitere Anknüpfungspunkte für die Berücksichtigung von Datenschutzbelangen. Die bisherige Diskussion sollte jedoch ausreichend verdeutlicht haben, dass in einer Unternehmenssituation, in der das IT-Servicemanagement nach ITIL durchgeführt wird, eine Berücksichtigung des Datenschutzes im ISM-Prozess sinnvoll ist, um den Vorgaben des BDSG nachzukommen, d. h. um sozusagen „BDSG-compliant" zu sein. Natürlich können die datenschutzrechtlichen Vorgaben auch parallel zu einem ISM-Prozess nach ITIL durch isolierte Maßnahmen umgesetzt werden – nur können bei einer solchen Trennung offensichtlich vorhandene Synergiepotenziale nicht genutzt werden. Eine getrennte Handhabung wäre mithin ineffizient.

2.2 Auftragsdatenverarbeitung

Auftragsdaten-verarbeitung

Mit der am 3. Juli 2009 vom Bundestag verabschiedeten BDSG-Novelle wurden u. a. Regelungen zur Auftragsdatenverarbeitung getroffen.[22] In § 11 Abs. 1 Satz 1 BDSG wird klargestellt, dass auch bei einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch beauftragte Dritte die Verantwortung für die Einhaltung der Vorgaben des BDSG beim beauftragenden Unternehmen verbleibt. Um diese Verantwortung wahrzunehmen, müssen bei der Beauftragung eines IT-Dienstleisters verschiedene datenschutzrelevante Aspekte, die in § 11 Abs. 2 Satz 2 BDSG nicht abschließend aufgeführt sind, vertraglich geregelt werden.

Bezug auf § 9 BDSG

Ein enger Bezug zwischen ITIL und den Regelungen des § 11 BDSG besteht schon deshalb, weil § 11 Abs. 4 Satz 1 Nr. 2 BDSG mit der Geltung von § 4 g BDSG indirekt und § 11 Abs. 2 Satz 2 Nr. 3 BDSG direkt auf die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen als Regelungstatbestand verweist, vgl. die Verweisungsstruktur in Abbildung 2. Damit treffen auch aus Sicht der Auftragsdatenverarbeitung die im vorherigen Abschnitt beschriebenen Zusammenhänge bezüglich der Informationssicherheit zu.

---

[21] Nach *Sowa 2008*, S. 81.

[22] *Hoeren* weist jedoch darauf hin, dass viele der Verpflichtungen des § 11 Abs. 2 Satz 2 BDSG auch schon vor Verabschiedung des Gesetzes dadurch bestanden haben, dass Aufsichtsbehörden den Unternehmen bzw. den betrieblichen Datenschutzbeauftragten entsprechende Verpflichtungen auferlegt haben, s. *Hoeren 2010*, S. 688.

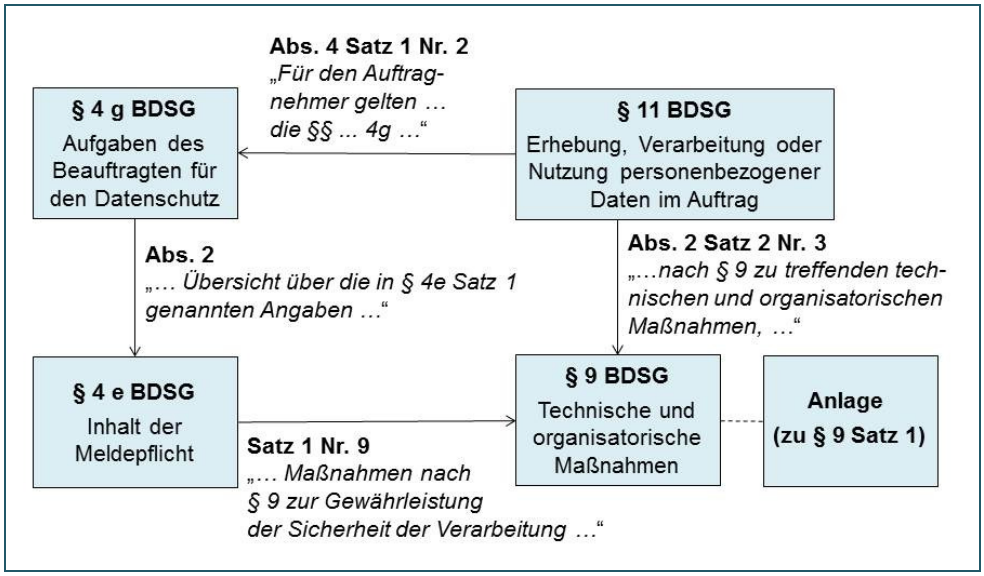

Abbildung 2
BDSG-Paragrafen zur Auftragsdatenverarbeitung und Informationssicherheit

Bezug zum Supplier Management

Neben dem engen Bezug zum Informationssicherheitsmanagement besteht jedoch ein mindestens ebenso enger Zusammenhang mit dem Lieferantenmanagement (Supplier Management). Dieser IT-Prozess ist wie der ISM-Prozess im Buch „Service Design“ beschrieben.[23] Die Vorgaben zur Auftragsdatenverarbeitung betreffen alle fünf Teilprozesse des Supplier Managements, vgl. Abbildung 3:

- Mit Blick auf den Datenschutz beinhaltet der Teilprozess „Evaluation of new suppliers & contracts“ eine lieferanten- bzw. vertragsbezogene Risikoanalyse, die rechtliche Risiken, insbesondere die im Folgenden genannten Bußgelder bei Verstoß gegen Vorgaben des BDSG, einbeziehen muss.[24]
- Im Rahmen des Teilprozesses „Establish new suppliers & contracts“ sind die Vorgaben aus § 11 Abs. 2 Satz 2 BDSG in den Vertrag mit dem Lieferanten aufzunehmen. Werden die nach § 11 Abs. 2 Satz 2 BDSG vorzunehmenden Regelungen nicht getroffen, droht ein Bußgeld nach § 43 Absatz 1 Satz 1 Nr. 2b BDSG i. V. m. § 43 Absatz 3 Satz 1 BDSG in Höhe von bis zu 50.000,– €. Weiterhin ist die Vorgabe aus § 11 Abs. 2 Satz 2 Nr. 4 BDSG zu erfüllen. Hiernach hat sich der Auftraggeber vor (!) der Ausführung des Auftrags von den „beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“. Wird dieser Pflicht nicht nachgekommen, so droht nach

[23] Siehe *ITIL SD 2007*, S. 149-164.
[24] Siehe *ebd.*, S. 154.

§ 43 Absatz 1 Satz 1 Nr. 2b BDSG i. V. m. § 43 Absatz 3 Satz 1 BDSG ebenfalls ein Bußgeld in Höhe von bis zu 50.000,– €.

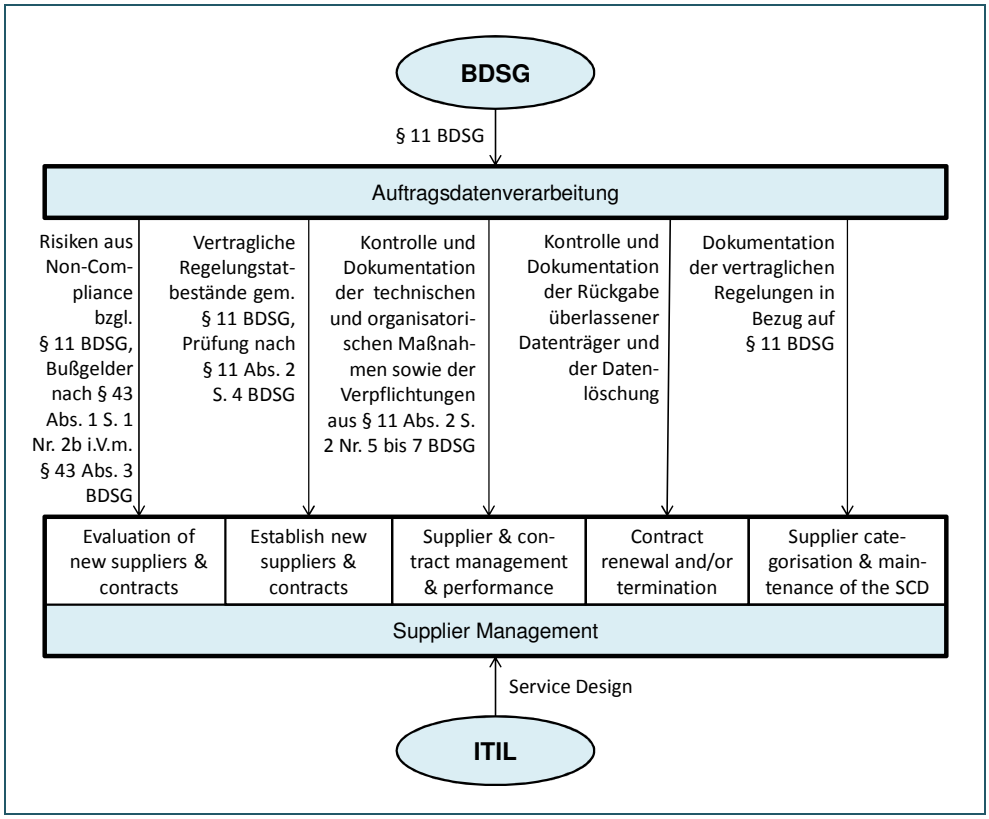

Abbildung 3
Zusammenhänge zwischen Auftragsdatenverarbeitung und Supplier Management

- Im Teilprozess „Supplier & contract management & performance“ muss den Vorgaben zur Auftragsdatenverarbeitung nachgekommen werden. Die Erfüllung ist zu kontrollieren und zu dokumentieren. Im Einzelnen fallen folgende Aufgaben an: Die Kontrolle der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen ist auch während der Auftragsdurchführung eine kontinuierliche Pflicht des Auftraggebers. Ebenso ist vom Auftraggeber die Einhaltung der sich aus den § 11 Abs. 2 Satz 2 Nr. 5 bis 7 BDSG ergebenden Verpflichtungen des Lieferanten[25] zu kontrollieren.
- Im Teilprozess „Contract renewal and/or termination“ ist die Vertragsbeendigung betroffen. Nach § 11 Abs. 2 Satz 2 Nr. 10 BDSG hat der Vertrag „die Rückgabe überlassener Datenträger und die Löschung

[25] Diese beziehen sich auf vorzunehmende Kontrollen (Nr. 5), die Begründung von Unterauftragsverhältnissen (Nr. 6) sowie Duldungs- und Mitwirkungspflichten des Auftragnehmers bei Kontrollen durch den Auftraggeber (Nr. 7).

beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags“ zu regeln. Die getroffenen Regelungen sind bei Vertragsbeendigung zu erfüllen und die tatsächliche Durchführung ist i. S. der Beweisbarkeit zu dokumentieren.

- Im Teilprozess „Supplier categorisation & maintenance of the SCD“ sind die getroffenen vertraglichen Regelungen zur Auftragsdatenverarbeitung in der Lieferanten- und Vertragsdatenbank, der „Supplier and Contract Database“ (SCD) zu dokumentieren.

Beteiligung DSB

Praktisch ist es also unumgänglich, die BDSG-Vorgaben in den sach-logischen Ablauf des gesamten Lieferantenmanagement-Prozesses zu integrieren. Dies bedeutet nicht nur, die entsprechenden Aufgaben vorzusehen und durchzuführen, sondern auch diesbezüglich den Datenschutzbeauftragten entsprechend zu beteiligen.

2.3 Zusammenfassung der gegenseitigen Bezüge

Bisherige Gegenüberstellung

Die bisherige Erörterung stellte die Anforderungen hinsichtlich der Auftragsdatenverarbeitung und der zu ergreifenden technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes den beiden ITIL-spezifischen IT-Prozessen „Information Security Management“ und „Supplier Management“ gegenüber, siehe Abbildung 4.

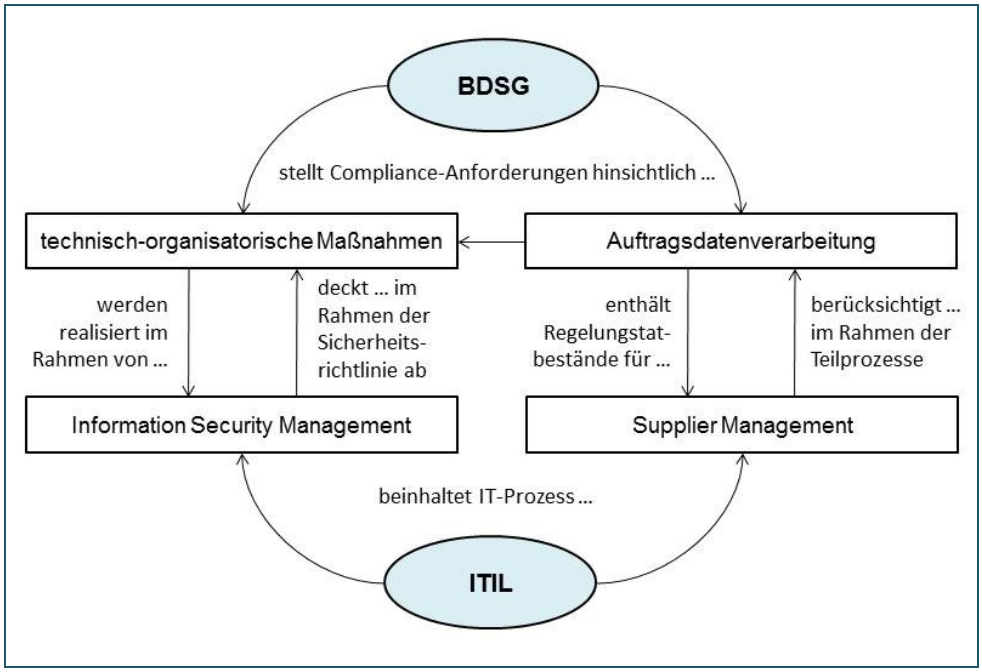

Abbildung 4
Ausgewählte Zusammenhänge zwischen BDSG und ITIL

Zwei grundlegende Perspektiven

Wie gezeigt erweisen sich vor allem zwei Perspektiven als grundlegend für eine Integration des Datenschutzes in die beiden diskutierten ITIL-spezifischen IT-Prozesse.

- Als Gesetz findet das BDSG notwendig Berücksichtigung in ITIL. An vielen Stellen wird dort darauf hingewiesen, dass gesetzliche und regulatorische Vorgaben als Anforderungen an Informationen, Prozesse etc. identifiziert und umgesetzt werden müssen.
- Aus den im BDSG enthaltenen detaillierten Anforderungen ergeben sich enge sach-logische Zusammenhänge mit den diskutierten Prozessen.

Begründung der Integration

Aus Gründen der Effektivität und der Effizienz ist es somit geboten, die Umsetzung des Datenschutzes, vor allem des BDSG, nicht parallel zu den ITSM-Strukturen des Unternehmens zu verfolgen, sondern diese zum beiderseitigen Vorteil in ein an ITIL orientiertes IT-Servicemanagement zu integrieren.[26] Entscheidend ist der Umfang der aus den Zusammenhängen resultierenden Bezüge zwischen Datenschutz und ITIL. Gesetzliche Anforderungen ergeben sich auch aus anderen Rechtsnormen (Gesetzen, Verordnungen etc.) sowie aus der Rechtsprechung. Auch diese müssen Eingang in das IT-Servicemanagement finden. Allein die Vielzahl der Vorgaben und der sach-logischen Zusammenhänge sowie die gesetzlich vorgeschriebene Position des betrieblichen Datenschutzbeauftragten erfordern eine umfangreiche, ausdrückliche und systematische Integration des Datenschutzes in ITIL. Wie diese Integration genauer ausgestaltet sein kann, ist Inhalt des folgenden Kapitels.

3. Ansatzpunkte für eine Integration des Datenschutzes in ITIL

Zielsetzung

Bisher wurde noch eher allgemein bzw. anhand von Beispielen vom Zusammenhang zwischen Datenschutz und ITIL gesprochen. Im letzten Abschnitt

[26] So im Wesentlichen auch der „ISACA-Leitfaden zur Auftragsdatenverarbeitung unter Berücksichtigung von Standards“. Hier wird ein Mapping zwischen dem § 11 BDSG und der ISO/IEC 27001:2005 vorgenommen. Die Verfasser kommen zu dem Ergebnis, dass es sinnvoll ist, dass „Prüfungshandlungen, die im Rahmen der Verpflichtung des § 11 BDSG vorgenommen werden, im Einklang mit den Anforderungen der ISO 27001 stehen, um Synergieeffekte zu erzielen und Doppelarbeiten sowie Akzeptanzprobleme beim Auftragnehmer zu vermeiden“ (*ISACA 2011*, S. 30).

des zweiten Kapitels wurden zwei grundlegende Perspektiven identifiziert: gesetzliche Anforderungen und sach-logische Zusammenhänge, die beide in den ITIL-spezifischen Prozessen zu berücksichtigen sind. In diesem Kapitel sollen diese und weitere Ansatzpunkte für eine systemische Integration des Datenschutzes in ITIL betrachtet werden, siehe Abbildung 5.

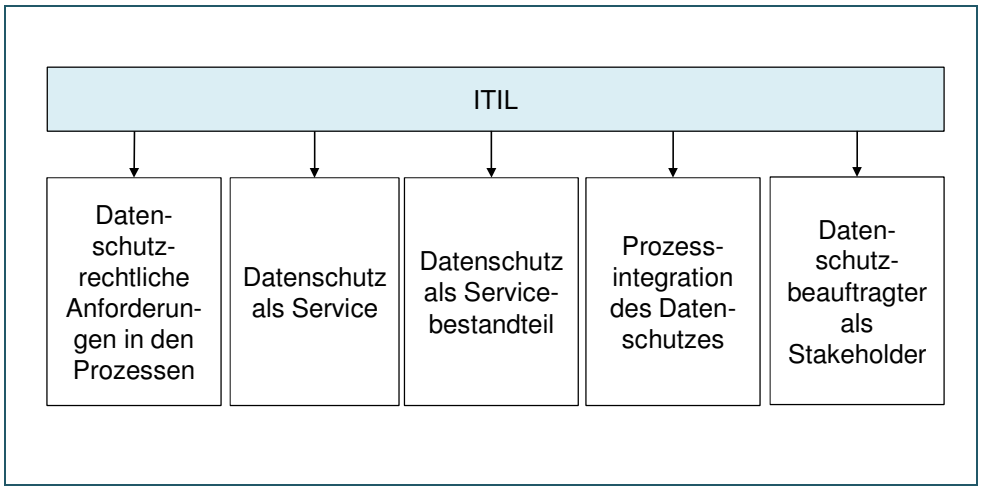

Abbildung 5
Ansatzpunkte für eine Integration des Datenschutzes in ITIL

Ansatzpunkte

- Eine unabweisbare Integrationsnotwendigkeit besteht dort, wo datenschutzrechtliche Anforderungen in den ITIL-Prozessen zu berücksichtigen und umzusetzen sind. Hieraus ergibt sich allerdings nur eine eher beiläufige Integration, die grundsätzlich für jede rechtliche Anforderung gilt und somit keine herausgehobene Position des Datenschutzes rechtfertigt.
- Demgegenüber würde die weitgehendste Integration des Datenschutzes in ITIL darin bestehen, dass Datenschutz einen eigenen IT-Service bildet.
- Statt eines eigenen Services könnte Datenschutz auch als spezieller Servicebestandteil ausdrücklich in andere IT-Services einbezogen werden.
- Wenn diese weitgehende Integration nicht gewünscht wird, so ist zumindest eine sach-logische Integration in die ITIL-Prozesse erforderlich. Diese prozessuale Integration erfordert die passgenaue Einbeziehung des Datenschutzes in die einzelnen ITSM-Verfahrensabläufe nach ITIL.
- Aus den vorangegangenen Punkten resultiert die Teilhabe des DSB als Stakeholder der ITIL-Prozesse.

Diese fünf Ansatzpunkte sollen im Folgenden eingehend diskutiert werden. Die Erörterung beginnt mit den an die ITIL-Prozesse gerichteten Anforderungen, die aus datenschutzgesetzlichen Vorgaben resultieren

3.1 Datenschutzgesetzliche Anforderungen in den ITIL-Prozessen

Berücksichtigung gesetzlicher/regulatorischer Vorgaben

In den verschiedensten Prozessen der vier Domänen Service Strategy, Service Design, Service Transition und Service Operation wird immer wieder auf die Notwendigkeit der Berücksichtigung gesetzlicher und regulatorischer Vorgaben hingewiesen. Die aus Datenschutzgesetzen (BDSG, TKG, TMG, Landesdatenschutzgesetze) resultierenden Anforderungen bilden hier eine Teilmenge der gesetzlichen und regulatorischen Vorgaben. An dieser Stelle sollen lediglich die Anforderungen des BDSG betrachtet werden, da sich dieses gleichermaßen an alle Unternehmen und öffentliche Einrichtungen richtet. Tabelle 2 listet die ausdrücklichen Verweise auf gesetzliche und regulatorische Anforderungen in den ITIL-Prozessen der vier Domänen auf.

Tabelle 2
Verweise auf gesetzliche und regulatorische Anforderungen in ITIL-Prozessen

Domäne/ Abschnitt	Prozess	Bezug
SS 5.3.1	Service Portfolio Management	Im Rahmen der Priorisierung von Investitionen sollen neben finanziellen Kriterien auch andere Faktoren berücksichtigt werden. Als einer dieser Faktoren ist auch „legal compliance“ zu berücksichtigen.
SD 4.6.2	Information Security Management	Für die Richtlinie zur Informationssicherheit ist ein umfassendes Verständnis des Sicherheitumfeldes wichtig. Hierzu gehören auch die externen gesetzlichen Anforderungen.
SD 4.7.5.1	Supplier Management	Eine im Vorfeld einer vertraglichen Regelung vorzunehmende Risikoanalyse hat sich auch auf relevante gesetzliche Vorgaben zu erstrecken.
ST 4.1.5.1	Transition Planning and Support	Für die Überführung von Services in den Wirkbetrieb ist eine Überführungsstrategie zu entwickeln, die auch gesetzliche Anforderungen zu berücksichtigen hat.
ST 4.2.3	Change Management	Ein effektives Change Management trägt dazu bei, sich ändernde gesetzliche und regulatorische Vorgaben zu erfüllen.
ST 4.3.4.1	Service Asset and Configuration Management	SACM-Grundsätze (Service Asset and Configuration Management) basieren u. a. auf gesetzlichen und regulatorischen Vorgaben. … Als IT Assets stehen Hard- und Softwarelösungen im Vordergrund, durch die gesetzliche und regulatorische Compliance erreicht werden kann.

Domäne/ Abschnitt	Prozess	Bezug
ST 4.3.4.2		Organisations-CIs (Configuration Item) können sich auch auf regulatorische Anforderungen richten.
ST 4.4.5.1	Release and Deployment Management	Vor der Überführung eines Service in den Wirkbetrieb sind Kriterien festzulegen, nach denen Erfolg oder Misserfolg der Überführung beurteilt werden können. In diese Kriterien gehen auch regulatorische Vorgaben ein.
ST 4.5.4.10	Service Validation and Testing	Der Test von Services umfasst auch nicht-funktionale Tests. Diese richten sich auch auf regulatorische Anforderungen.
ST 4.7.3	Knowledge Management	Das Knowledge Management hat sich auch auf gesetzliche Anforderungen zu richten, die z. B. bei der Überführung von Services in den Wirkbetrieb zu berücksichtigen sind.
ST 4.7.5.3	Knowledge Management	Knowledge Management hat Informationen zu gesetzlichen Anforderungen und zur aktuellen Gesetzgebung einzubeziehen und diesbezügliche Entwicklungen zu beobachten.
SO 4.2.5.4	Incident Management	Bei der Bewertung der Auswirkungen eines Incident sind auch die Folgen von Verstößen gegen gesetzliche und regulatorische Vorgaben zu berücksichtigen.
SO 4.5.3	Access Management	Access Management stellt u. a. die Erfüllung gesetzlicher und regulatorischer Vorgaben sicher.

Mitunter wird in den Prozessbeschreibungen sogar explizit Bezug auf datenschutzrechtliche Vorgaben genommen. Tabelle 3 listet die ausdrücklichen Verweise auf den Datenschutz in den verschiedenen ITIL-Domänen und -Prozessen auf.

Domäne/ Abschnitt	Prozess	Bezug
SD 4.6.5	Information Security Management	Datenschutz erfährt eine zunehmende Bedeutung und zeigt sich vermehrt in regulatorischen Aktivitäten des Gesetzgebers. Technologien, die die Einhaltung der daraus resultierenden Vorgaben unterstützen, werden damit zunehmend wichtiger.
ST 4.5.4.9 4.5.7	Service Validation and Testing	Die Nutzung personenbezogener Testdaten hat gesetzliche Datenschutzvorgaben zu berücksichtigen. Entsprechendes gilt für die Pflege personenbezogener Testdaten.

Tabelle 3
Verweise auf datenschutzrechtliche Anforderungen in ITIL-Prozessen

Domäne/ Abschnitt	Prozess	Bezug
ST 4.7.5.3	Knowledge Management	Das Informationsmanagement hat Anforderungen des Datenschutzes als beschränkende Bedingungen zu berücksichtigen.
SO 4.5.7.2	Access Management	Personenbezogene Daten unterliegen in vielen Ländern datenschutzrechtlichen Bestimmungen. Ihr Schutz sollte im Rahmen der Sicherheitsverfahren des Unternehmens erfolgen.

Diese Bezüge stellen mithin das Minimum der Integration des Datenschutzes in ein IT-Servicemanagement nach ITIL dar. Dort, wo ITIL genutzt wird, sollte der DSB zumindest an diesen Stellen in unterschiedlichem Ausmaß (vgl. Abschnitt 3.5) beteiligt sein.

3.2 Datenschutz als Service

Begriff „IT-Service“

Grundlegend für das ITIL-Framework ist der Begriff des IT-Service. Hier stellt sich die Frage, ob Datenschutz nicht auch als ein IT-Service interpretiert werden kann, der in den Service-Katalog Eingang findet und vom Datenschutzbeauftragten verantwortet wird. Nach ITIL ist ein Service „a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks“.[27]

Wertschöpfung durch Service

Ein wesentliches Element des Serviceverständnisses ist die Wertschöpfung, die durch einen Service für den Kunden kreiert wird. ITIL enthält hierfür ein generisches, zweigliedriges Wertschöpfungsmodell, wonach die zu erbringende Dienstleistung den Zweck („utility“) in einer geeigneten Form („warranty“) erfüllen muss.

- Der Zweck wird dann erreicht, wenn Nutzen entsteht, d. h. die Leistungsfähigkeit des Kunden direkt unterstützt wird oder Beschränkungen der Leistungsfähigkeit beseitigt werden.
- Die Form des Service bezieht sich auf die Anforderungen der Verfügbarkeit, der Kapazität, der Kontinuität und der Sicherheit, die alle in erforderlichem Ausmaß gewährleistet sein müssen.[28]

[27] *ITIL SS 2007*, S. 16.
[28] Nach *ebd.*, S. 17; vgl. Johannsen/Goeken, die den Formaspekt als „garantierte Verlässlichkeit“ bezeichnen und darunter verstehen, dass ein Service „dauerhaft und sicher sowie mit ausreichender Kapazität verfügbar sein muss“ (*Johannsen/Goeken 2011*, S. 200).

Die beiden Zweige (warranty und utility) müssen gleichzeitig erfüllt sein, um eine Wertschöpfung des Service zu generieren. Für die reale Umsetzung dieser Anforderungen werden so genannte „Service Level Packages“ (SLPs) definiert, die für unterschiedliche Leistungsklassen verschiedene Service-Komponenten kombinieren. Dabei setzt sich ein Warranty-SLP aus einzelnen SLPs für jede der Anforderungen Verfügbarkeit, Kapazität, Kontinuität und Sicherheit zusammen. So wird als Beispiel für ein Security-SLP eine Kombination der Servicekomponenten tokenbasiertes Authentifizierungsverfahren, Security-Token (Hardware), Virtual Private Network (VPN) und Secure FTP angeführt.[29]

Spezielle Datenschutzservices?

In dieser allgemeinen Auffassung ist es durchaus vorstellbar, die Leistungen des betrieblichen Datenschutzes[30] als Services i. S. von ITIL zu definieren. Die verschiedenen Datenschutzservices gewährleisten ein Schutzniveau entsprechend den gesetzlichen Anforderungen oder erfüllen gesetzlich vorgeschriebene Aufgaben, schaffen also für den „Kunden“ einen entsprechenden Nutzen. Dies entspricht dem Utility-Zweig des Wertschöpfungsmodells. Aber auch der Warranty-Zweig lässt sich auf Datenschutzservices beziehen. Diese müssen für diejenigen Geschäftsprozesse, in denen personenbezogene Daten verarbeitet werden, verfügbar sein und kontinuierlich in ausreichender Kapazität erbracht werden. Auch die Tatsache, dass Datenschutzservices überwiegend einen eher geringen hard- und softwaretechnischen Anteil haben dürften, spricht nicht prinzipiell gegen eine Sichtweise von Datenschutzleistungen als IT-Service i. S. von ITIL.

Ablehnung der Sichtweise

Wenn dieser Auffassung trotzdem nicht gefolgt werden soll, so liegt dies an dem oben beschriebenen grundlegenden Verständnis eines Service, der einem Kunden eine Risikoabwälzung erlauben soll („without the ownership of specific … risks“). Gerade eine solche Risikoabwälzung darf im Falle des Datenschutzes nicht möglich sein. Zwar obliegt der Unternehmensleitung in Bezug auf die Gewährleistung des Datenschutzes die Letztverantwortung. Wirksam umgesetzt werden kann Datenschutz jedoch nur dann, wenn die Verantwortung durch Delegation dezentralisiert und operativ von denjenigen Stellen wahrgenommen wird, die unmittelbar mit personenbezogenen Daten umgehen. Bereits die Position des DSB führt mitunter zu der Ein-

[29] Nach *ITIL SS 2007*, S. 135f.
[30] Bspw. die Durchführung von Mitarbeiterschulungen zu Datenschutzfragen, die Vorabkontrolle bei automatisierten Verarbeitungen oder die Mitwirkung bei der Beantwortung von Auskunftsersuchen von Betroffenen.

stellung, dass es doch mit dem DSB eine verantwortliche Stelle für den Datenschutz gibt – mit der Folge, dass eine eigene Verantwortung wenn schon nicht abgelehnt, dann doch zumindest marginalisiert wird. Die Risiken mangelnden Datenschutzes müssen von den ausführenden Mitarbeitern erkannt und akzeptiert werden und sie müssen entsprechend sensibilisiert die Anforderungen des Datenschutzes in ihrem Aufgabenbereich erkennen, umsetzen und ihre Einhaltung verantworten. Die Inanspruchnahme von Datenschutzservices würde dieser dezentralisierten Verantwortung widersprechen.

Wenn Leistungen des Datenschutzes schon nicht als spezielle Datenschutzservices ausgestaltet sein sollen, so können sie doch eventuell zumindest einen Bestandteil eines IT-Service bilden. Diese Sichtweise soll im nächsten Abschnitt diskutiert werden.

3.3 Datenschutz als Servicebestandteil

Datenschutz als Servicekomponente

Datenschutz als einen Servicebestandteil zu interpretieren bedeutet, Leistungen des Datenschutzes als Servicekomponente anzusehen. Hierzu sind zwei Varianten denkbar:

- Zum einen kann Datenschutz als eigene Anforderung eines IT-Service verstanden werden. In diesem Fall würde die Datenschutzanforderung ein eigenes Warranty-SLP, d. h. ein Datenschutz-Service Level Package, darstellen.
- Zum anderen können Datenschutzanforderungen als Teil der Sicherheitsanforderung eines Service eingestuft werden, so dass die Datenschutzanforderungen durch die Servicekomponenten des Security-SLP erfüllt werden.

Eigener Datenschutz-SLP

Der Ansatz, Leistungen des Datenschutzes als eigenes Datenschutz-SLP, das wiederum Teil eines übergeordneten Service Level Packages ist, zu konstruieren, soll am Beispiel der Nutzung eines Notebooks mit einer portablen Festplatte demonstriert werden: Ein im Außendienst tätiger Nutzer benötigt für seine portable Gerätschaft eine Rund-um-die-Uhr-Verfügbarkeit bei weltweitem Einsatz. Aufgrund der auf dem Gerät gespeicherten personenbezogenen Daten wird ein hohes Schutzniveau benötigt, so dass fortgeschrittene Zugangs- und Zugriffskontrollen verwendet werden müssen. Diese Anforderungen lassen sich nun in einem eigenen Datenschutz-SLP bündeln. Das entsprechende Service Level Package ist in Abbildung 6 dargestellt.

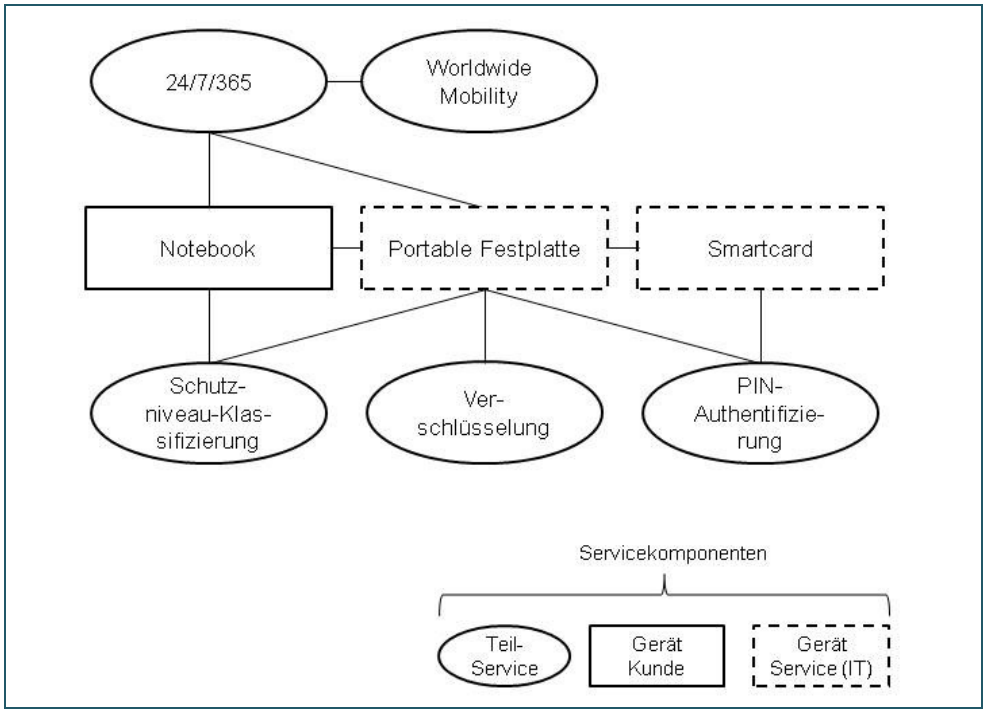

Abbildung 6
Datenschutz-SLP als Kombination verschiedener Service-komponenten[31]

Falls das benötigte Schutzniveau entsprechend einer Schutzniveauklassifizierung niedriger sein oder ein Teilservice weniger umfangreich erbracht werden kann, könnte dieses SLP nach Zielgruppen differenziert werden. Als Datenschutz-SLP würde das SLP durch den Bereich Datenschutz verantwortet werden. Dieser bzw. der Datenschutzbeauftragte in Person wäre dann als (eine unter mehreren) „specialized group" im Rahmen von ITIL anzusehen, die zum Management eines gesamten SLP über spezifische Fähigkeiten und Ressourcen verfügt.[32]

Datenschutz als Teil des Security-SLP

Als Alternative zu einem eigenen Datenschutz-SLP können Datenschutzanforderungen auch durch die Servicekomponenten des Security-SLP erfüllt werden. Dieser Ansatz hat seine Berechtigung dadurch, dass es nur schwer vorstellbar ist, dass es originäre Servicekomponenten für den Datenschutz gibt, die nicht zugleich auch Sicherheits-Servicekomponenten darstellen. Dies dürfte insbesondere für die vom BDSG geforderten Kontrollen gelten.

Kein gegenseitiger Ausschluss

Beide Ansätze schließen sich nicht gegenseitig aus. Der Unterschied besteht vor allem in einer unterschiedlichen Verantwortung der für den Datenschutz verantwortlichen Stelle, d. h. der Rolle des Datenschutzbeauftragten.

[31] Vgl. die Abbildung in *ITIL SS 2007*, S. 136.
[32] Vgl. *ebd.*, S. 137.

- Bei speziellen Datenschutz-SLPs hat dieser eine höhere Verantwortung durch die Eigentümerschaft in Bezug auf das SLP, wobei sich diese Verantwortung nicht notwendig auf den Betrieb von Hard- und Software erstrecken muss. Im obigen Beispiel kann der DSB für die Datenschutzklassifizierung und die Ausgestaltung der hard- und softwaretechnischen Komponenten verantwortlich sein, während der Betrieb, d. h. die operative Umsetzung der Anforderungen in hard- und softwaretechnische Komponenten, in den Händen der IT-Abteilung liegen kann.
- Bei der Berücksichtigung der Datenschutzanforderungen im Rahmen eines Security-SLP liegt die Eigentümerschaft in Bezug auf das SLP bei der IT-Funktion. Der DSB hat in diesem Fall nur für die Definition der Anforderungen und die Kontrolle der Realisierung zu sorgen. In dieser Sichtweise ist er lediglich ein zu beteiligender Stakeholder.

Eine weitere Möglichkeit der Integration des Datenschutzes in ein IT-Servicemanagement nach ITIL bildet die Integration von Aufgaben und Abläufen des Datenschutzes in die verschiedenen ITIL-Prozesse. Diese prozessuale Integration soll im nächsten Abschnitt diskutiert werden.

3.4 Prozessintegration des Datenschutzes

Sach-logische Integration

Wie Datenschutz in einen Prozess sach-logisch integriert werden kann bzw. muss, wurde bereits exemplarisch anhand des Prozesses „Supplier Management“ (siehe Abschnitt 2.2) beschrieben. In einer allgemeineren Betrachtung gibt es drei wesentliche Ansatzpunkte für eine prozessuale Integration des Datenschutzes in die ITIL-Prozesse: die Berücksichtigung des Datenschutzes als Aufgabeninhalt oder als Prozessanforderung sowie im Zusammenhang mit der Nutzung von Tools, die die Prozessdurchführung unterstützen, vgl. Abbildung 7.

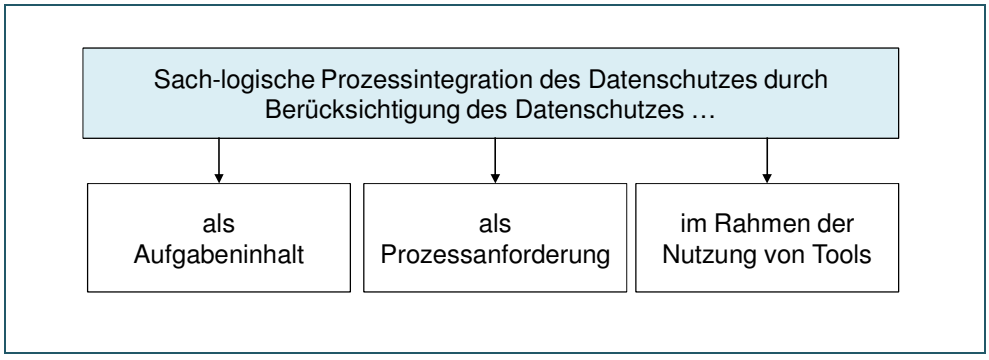

Abbildung 7
Prozessuale Integration des Datenschutzes

Diese drei Formen der prozessualen Integration des Datenschutzes in die ITIL-Prozesse werden im Folgenden beschrieben.

3.4.1 Prozessintegration als Aufgabeninhalt

DS als Aufgabeninhalt

Die Umsetzung datenschutzgesetzlicher Vorgaben kann Teil der verschiedenen Aufgaben sein, aus denen ein ITIL-Prozess besteht. Datenschutz wird hier zum Aufgabeninhalt. Folgende Beispiele sollen diese Form der Integration verdeutlichen:

- Im Prozess „Supplier Management“ sind bei Auftragsdatenverarbeitung Regelungstatbestände nach § 11 BDSG in die Vertragsgestaltung einzubeziehenden, Kontrollen der technisch-organisatorischen Maßnahmen und der sonstigen Verpflichtungen nach § 11 BDSG im Rahmen des Lieferanten- und Vertragsmanagements vorzunehmen sowie die Rückgabe überlassener Datenträger bzw. die Durchführung der Datenlöschung im Rahmen der Vertragsbeendigung zu kontrollieren.
- Im Rahmen des Prozesses „Service Validation and Testing“ stellt das „Regulatory and Compliance Testing“ einen nicht-funktionalen Test dar, mit dem die Konformität u. a. mit gesetzlichen Vorgaben sichergestellt werden soll.[33]
- Datenschutzgesetzliche Vorgaben können Teil von Risikoanalysen sind, die in verschiedenen ITIL-Prozessen angestellt werden. Im Prozess „Supplier Management“ wären im Falle einer Auftragsdatenverarbeitung in der vorvertraglichen Risikoanalyse[34] datenschutzrechtliche Belange zu berücksichtigen. Auch im Change Management spielt die Analyse von Risiken aus Gesetzesverstößen eine Rolle bei der Überführung neuer Releases in den Betrieb.

Verstoß gegen DS als Spezialfall

Als Spezialfall eines datenschutzrelevanten Aufgabeninhalts können Tätigkeiten angesehen werden, deren Ausführung zu einem Verstoß gegen datenschutzgesetzliche Vorgaben führen kann. Ein Beispiel hierfür wäre die Auswertung von Systemdaten im Rahmen des Incident Managements. Im Grundsatz ist wohl davon auszugehen, dass diese Protokolldaten notwendig auch personenbezogene Daten umfassen. Allerdings ist die Protokollierung personenbezogener Daten aus Gründen der gebotenen Datensparsamkeit ge-

[33] Vgl. *ITIL ST 2007*, S. 128ff.
[34] Nach *ITIL SD 2007*, S. 154.

mäß § 3a BDSG auf ein Minimum zu begrenzen. Für die Zwecke des Incident Managements sind sie zumindest zu anonymisieren oder zu pseudonymisieren.[35]

3.4.2 Prozessintegration als Prozessanforderung

DS als Teil der Prozess-anforderungen

Als Teil gesetzlicher und regulatorischer Vorgaben sind die datenschutzgesetzlichen Vorgaben häufig Teil der Anforderungen, die im Rahmen der Prozessdurchführung zu berücksichtigen sind. Dies betrifft beispielsweise die Prozesse „Change Management“[36], „Service Level Management“ (SLM)[37] oder „Information Security Management“[38]. In einer umfassenderen Sichtweise können gesetzliche und regulatorische Vorgaben – da sie in der Durchführung der Geschäftsprozesse operativ umzusetzen sind – auch als Teil der Geschäftsanforderungen aufgefasst werden. Dann wären sie beispielsweise im Rahmen des Prozesses „Service Level Management“ und speziell in der Ausgestaltung der Service Level Agreements (SLA) zu berücksichtigen.[39]

DS als Ausprägung von Prozess-elementen

Die Integration des Datenschutzes als Ausprägung von Prozesselementen beruht darauf, dass es in vielen ITIL-Prozessen zentrale Handlungsobjekte gibt, auf die sich die Prozessdurchführung richtet. Datenschutz als Teil dieser Handlungsobjekte bedeutet, dass Datenschutzbelange als spezifischer Fokus in der Bearbeitung des Objektes berücksichtigt werden oder konzeptionell in das Objekt eingehen. Häufig wird die Bearbeitung des Objekts instrumentell durch Formulare oder Workflows unterstützt. Das Ergebnis der Bearbeitung enthält dann datenschutzrelevante Elemente als Teil einer Dokumentation oder Inhalt eines Systems.

Für die folgende detaillierte Betrachtung werden nur diejenigen ITIL-Prozesse ausgewählt, die eine wesentliche Verbreitung in Unternehmen erfahren haben. Hierbei handelt es sich primär um die operativ orientierten ITIL-Prozesse, insbesondere der Domäne „Service Operation“.

---

[35] In Anlehnung an *Dolle 2005*, der explizit darauf hinweist, dass „das Erkennen eines Sicherheitsvorfalls nicht ohne die Erfassung und Auswertung von protokollierten Daten auskommt“, so dass „man sich beim Planen einer Incident-Response-Strategie auch zwangsläufig mit den geltenden Grundsätzen des Datenschutzes auseinandersetzen“ muss.
[36] Vgl. *ITIL ST 2007*, S. 45.
[37] Vgl. *ITIL SD 2007*, S. 65.
[38] Vgl. *ebd.*, S. 141.
[39] Vgl. *ebd.*, S. 65ff.

Tabelle 4 listet die wesentlichen IT-Prozesse und ihre datenschutzrelevanten Handlungsobjekte auf.[40]

Domäne	Prozess	Handlungsobjekt
SD	Service Level Management	Service Level Agreement (SLA) Operational Level Agreement (OLA) Service Level Requirement (SLR)
	Information Security Management	Information Security Policy (ISP)
ST	Change Management	Request for Change (RFC)
	Service Asset and Configuration Management	Configuration Item (CI)
SO	Event Management	Event
	Incident Management	Incident
	Request Fulfillment	Service Request
	Problem Management	Problem

Tabelle 4
IT-Prozesse mit wesentlichen datenschutzrelevanten Handlungsobjekten

… in der Domäne „Service Design“

In der Domäne „Service Design“ sind die Prozesse „Service Level Management“ und „Information Security Management“ betroffen:

- Im Rahmen des Prozesses „Service Level Management“ sind Service Level Agreements zu erstellen, die auch die Serviceziele und die Verantwortlichkeiten der das SLA vereinbarenden Parteien beinhalten.[41] Datenschutzbelange können hier als ein Regelungstatbestand eine Rolle spielen. In diesem Fall wären zudem sowohl die Verantwortlichkeiten des DSB im Rahmen eines Service als auch die Verantwortlichkeiten der Fachabteilung für den Datenschutz in Bezug auf die Nutzung des Service zu regeln. Gleiches gilt im Prinzip auch für die „Operational Level Agreements“ (OLA). Die Basis für die Vereinbarung der Serviceziele bilden sog. „Service Level Requirements“ (SLR) [42], in die gegebe-

[40] Die Auswahl der Prozesse richtete sich nach der Materna-Studie von 2010, siehe *Materna 2010*, S. 16. Die aufgeführten Prozesse sind in 71 % bis zu 97 % der in der Studie befragten Unternehmen zumindest initial implementiert; zusätzlich zu den hier genannten Prozessen wurde das Event Management aufgenommen. Dieser Prozess war in der zweiten ITIL-Version noch in das Incident Management integriert und wurde vermutlich deswegen von den in der der Materna-Studie befragten Unternehmen nicht als eigenständiger Prozess praktiziert.
[41] Vgl. *ITIL SD 2007*, S. 66.
[42] Vgl. *ebd.*, S. 69f.

nenfalls auch Compliance-Vorgaben aus dem Datenschutz eingehen können.

- Im Rahmen des Prozesses „Information Security Management“ ist eine “Information Security Policy“ (ISP) zu erstellen, die verschiedene Richtlinien enthält – auch zu den im BDSG genannten Kontrollen (z. B. Zugangs- und Zugriffskontrollen).[43] Insofern sollten Datenschutzbelange expliziter Teil der ISP sein. Auch eine spezielle Richtlinie zum Datenschutz als integraler Teil der Information Security Policy wäre vorstellbar.

… in der Domäne „Service Transition“

Auch in der Domäne „Service Transition“ sind die Prozesse „Change Management“ und „Service Asset and Configuration Management“ betroffen:

- Der Prozess „Change Management“ wird durch einen Initiator mittels eines formellen „Request for Change“ (RFC) in Gang gesetzt.[44] Insbesondere für Services, die personenbezogene Daten verarbeiten, könnte es in Bezug auf Datenschutzbelange einen speziellen DS-RFC geben, der auch durch den DSB initiiert werden kann. Zumindest sollte das RFC-Formular eine Stellungnahme abfordern, ob der Datenschutz von einer beantragten Änderung betroffen ist.
- Zahlreiche Aufgaben im Prozess „Service Asset and Configuration Management“ richten sich auf „Configuration Items“ (CIs). In ihrer Summe bilden CIs die Komponenten (z. B. Hard- und Software, Dokumentation, Personal), die für den Betrieb eines IT-Service erforderlich sind. Ihr Lebenszyklus wird durch das Configuration Management verwaltet.[45] Aus Sicht des Datenschutzes könnte es spezielle DS-CIs geben, die den Datenschutz sicherstellen (z. B. Anonymisierungsmechanismen). Allerdings beinhaltet ITIL auch Service-CIs. Als solche gibt es „Service Capability Assets“ (SCA), die Management, Organisation, Prozesse, Wissen und Menschen umfassen. All diese Punkte treffen auch auf den Datenschutz zu, so dass dieser insgesamt oder in seinen Elementen als SCA betrachtet werden kann. „Service Resource Assets“ stellen eine weitere Gruppe der Service-CIs dar. Hierzu zählen auch Daten, so dass personenbezogene Daten entsprechend als ein Service Resource Asset zu klassifizieren wären. Und auch „Organization CIs“

[43] Vgl. *ITIL SD 2007*, S. 142.
[44] Vgl. *ITIL ST 2007*, S. 50.
[45] Nach *ebd.*, S. 67.

bilden eine Gruppe der Service-CIs. Zu dieser Gruppe zählen gesetzliche und regulatorische Anforderungen, die als externe Produkte betrachtet werden und die im Rahmen des Konfigurationsmanagements zu verfolgen sind.[46] Die relevanten Datenschutzgesetze können insofern als eigenständige Organization CIs eingestuft werden.

… in der Domäne „Service Operation“

In der Domäne „Service Operation“ sind bis auf das „Access Management“ alle Prozesse betroffen:

- Das „Event Management“ nimmt seinen Ausgang mit der Meldung eines Events. Ein Event ist eine Zustandsänderung eines IT-Service oder eines Configuration Item. Events werden vor allem als Systemmeldung durch Überwachungstools identifiziert, die mögliche Störungen oder Ausnahmesituationen anzeigen.[47] Soweit die Zustandsänderungen datenschutzrelevant sind, könnte ein Event auch als spezielles DS-Event klassifiziert werden, z. B. für einen unberechtigten Zugriff auf personenbezogene Daten.
- Sind Events als Störung identifiziert, richtet sich das „Incident Management“ auf das Beseitigen einer akuten oder sich abzeichnenden Störung von IT-Services.[48] Auch hier sind datenschutzrelevante Incidents leicht vorstellbar, z. B. der erfolgte unberechtigte Zugang zu einer IT-Infrastruktur, die personenbezogene Daten verarbeitet.
- Im Rahmen des Prozesses „Request Fulfillment“ fordern Nutzer mittels eines „Service Request“ von der IT-Abteilung definierte, standardisierte IT-Leistungen an. Die mit diesen Leistungen verbundenen Änderungen sind von geringem Risiko, größerer Häufigkeit und geringen Kosten.[49] Wiederum lassen sich hier datenschutzrelevante Anfragen ausmachen, beispielsweise ein Antrag auf Änderung des Zugriffs auf Systeme, die personenbezogene Daten verarbeiten.
- Das „Problem Management“ richtet sich auf die proaktive und reaktive Identifizierung und Beseitigung von Problemen als Ursachen von Störungen.[50] Soweit sich diese Probleme auf datenschutzrelevante Daten, IT-Komponenten, -Systeme oder -Services beziehen, wären Probleme entsprechend zu klassifizieren („DS-Probleme“) und zu priorisieren.

[46] Nach *ITIL ST 2007*, S. 68.
[47] Nach *ITIL SO 2007*, S. 36.
[48] Nach *ebd.*, S. 46.
[49] Nach *ebd.*, S. 46.
[50] Nach *ebd.*, S. 58f.

Gleiches gilt für die in einer Datenbank geführten „Known Errors“, die ggf. als datenschutzrelevant oder als spezielle „DS Known Errors“ zu kennzeichnen wären.

3.4.3 Prozessintegration im Rahmen der Nutzung von Tools

ITSM-Tools

Die Ergebnisse vieler Prozesse werden sich in den ITSM-Tools, die diese Prozesse unterstützen, wiederfinden. Es kann sich um datenschutzrelevante Daten oder Dokumente handeln, die dort abgelegt sind, oder um Datenschutzmerkmale verschiedener Objekte, die in den Tools verwaltet werden. Tabelle 5 listet die grundsätzlich relevanten Tools auf.

Tabelle 5
IT-Prozesse und ITSM-Tools

Domäne	Prozess	ITSM-Tool	
SD	Information Security Management	Security Management Information System	
	Supplier Management	Supplier and Contract Database (SCD)	
ST	Change Management	Logging System (Service Management Tool)	
	Service Asset and Configuration Management	Configuration Management System (CMS)	
	Knowledge Management	Service Knowledge Management System	
SO	Event Management	Service Desk (Management) Tool	
	Incident Management		Incident Management Tool
	Request Fulfillment		
	Problem Management		Known Error Database (KEDB)
	Access Management	Directory Services	

Daraus, dass der Datenschutz auf die eben beschriebene Weise in den ITIL-Prozessen zu berücksichtigen ist, resultiert notwendig die Einbeziehung des DSB in die betreffenden ITIL-Prozesse. Welche Formen diese Einbeziehung haben kann, wird im folgenden Abschnitt diskutiert.

3.5 Einbindung des Datenschutzbeauftragten als Stakeholder

Neben den eben dargestellten Integrationsmöglichkeiten ergibt sich eine weitere Integration des Datenschutzes in ITL durch die Einbindung der Position des Datenschutzbeauftragten in den Prozessablauf. Die verschiedenen

Möglichkeiten der Einbindung sollen im Folgenden anhand des Lieferantenmanagements[51] (Supplier Management) diskutiert werden.

DSB als Stakeholder

Wird der DSB im Rahmen eines ITIL-Prozesses tätig, so kommt ihm die Stellung eines Stakeholders zu. ITIL verwendet den Stakeholder-Begriff ausdrücklich und in dem üblichen Verständnis als berechtigt interessierte Personengruppe. Deren Interesse bezieht sich nicht nur auf IT-Services, sondern auch auf IT-Projekte und organisatorische Belange und umfasst im Einzelnen Ziele, Aktivitäten, Ressourcen und Leistungen i. S. von Ergebnissen.[52] In diesem Sinne kommt der DSB zweifellos als Stakeholder der ITIL-Prozesse in Frage, wobei er die Interessen des Datenschutzes in unterschiedlicher Art und Weise wahrnehmen kann, siehe Abbildung 8.

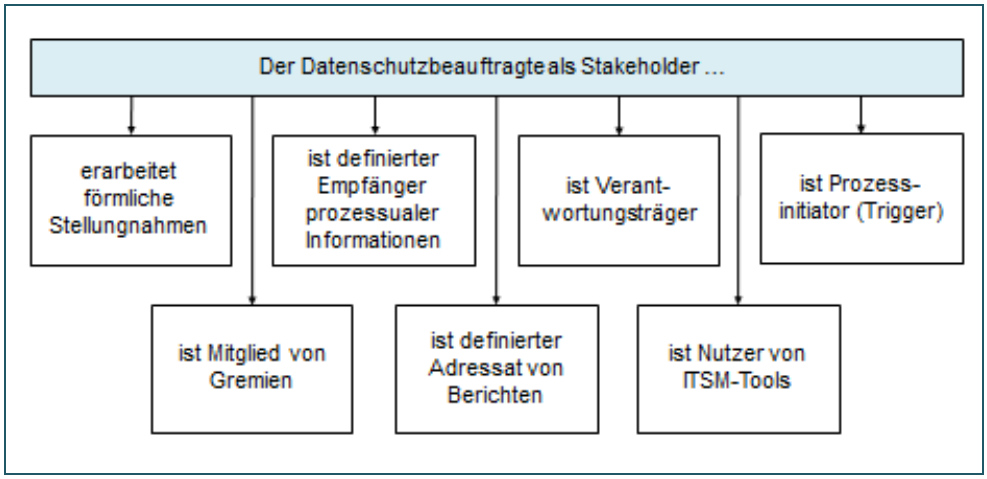

Abbildung 8
Der DSB als Stakeholder

Stellungnahme durch den DSB

In verschiedenen Aufgaben des Prozesses „Supplier Management“ ist eine Beurteilung aus Datenschutzsicht erforderlich. Diese sollte jeweils über eine geplante, formale Stellungnahme des DSB erfolgen. Im Einzelnen sollte der DSB Stellung nehmen bei

- der grundsätzlichen Ausgestaltung des Verfahrens zur Beauftragung neuer Lieferanten (inkl. Vertragsabschluss) sowie der Durchführung der Zusammenarbeit (insbesondere hinsichtlich der vorzunehmenden Reviews);
- der Kategorisierung des Lieferanten (insbesondere danach, ob eine Auftragsdatenverarbeitung vorliegt);

[51] Vgl. Abschnitt 2.2; vgl. im Folgenden *ITIL SD 2007*, S. 149-164.
[52] Nach *ITIL SS 2007*, S. 252.

- der Durchführung der Bewertungs- und Auswahlverfahren, der Vertragsgestaltung und der Leistung durch den Lieferanten i. S. einer Leistungsbewertung in Bezug auf datenschutzrelevante Bewertungskriterien;
- der Erstellung/Vereinbarung von Supplier Service Improvement Plans (SIPs), mit denen Verbesserungen in der Leistungserbringung des Lieferanten sowie in der gemeinsamen Zusammenarbeit erreicht werden sollen.
- der vorvertragliche Risikoanalyse; hier hat bei Vorliegen einer Auftragsdatenverarbeitung das Ergebnis der Prüfung der organisatorisch-technischen Maßnahmen des Lieferanten nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG Eingang zu finden;
- der Aktualisierung von Risikoanalysen während der Vertragsdurchführung.

Mitgliedschaften des DSB

Im Rahmen der Projektdurchführung ist der DSB mitunter Mitglied von Gremien und Arbeitsgruppen. Zum Zwecke der Leistungsbewertung finden in der Durchführung der Zusammenarbeit Reviews statt. Aus Sicht des DSB sind das „Supplier Performance Review“ und das „Contract Review“ relevant, da in beiden Fällen eine Bewertung auch aus Sicht des Datenschutzes erfolgen sollte bzw. muss (wiederum gemäß nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG). Der DSB sollte hier nach Möglichkeit Mitglied des jeweiligen Review-Teams sein.

DSB als Informationsempfänger

Als definierter Empfänger von Informationen sollte der DSB informiert werden, wenn datenschutzrelevante Inhalte der Supplier and Contract Database (SCD) erfasst oder verändert werden oder wenn Vertragsänderungen vorgenommen werden sollen. Weiterhin muss er eine Information erhalten, wenn im Falle einer Auftragsdatenverarbeitung eine Vertragsbeendigung ansteht.

DSB als Adressat von Berichten

Entsprechend seiner Beteiligung am gesamten Prozess des Lieferantenmanagements ist der DSB in das prozessbezogene Berichtswesen zu integrieren. Hierzu sollte er neben den Protokollen der Review-Meetings folgende Berichte zu erhalten:

(1) Supplier and Contract Performance Reports;

(2) Supplier Service Improvement Plans;

(3) Supplier Survey Reports.[53]

DSB als Verantwortungsträger

Bei Vorliegen von Auftragsdatenverarbeitung ist der DSB mehr als ein reiner Informationsempfänger – er wird zum Verantwortungsträger, wobei sich seine Verantwortung auf die Durchführung und/oder das Ergebnis eines Prozesses erstrecken kann. Im Rahmen des Lieferantenmanagements hat der DSB folgende Aufgaben verantwortlich wahrzunehmen:

(4) Freigabe des zu unterzeichnenden Vertrages in Bezug auf die datenschutzgesetzlichen Regelungstatbestände nach § 11 BDSG;

(5) Freigabe von Supplier Service Improvement Plans, soweit datenschutzrelevante Änderungen vereinbart werden sollen;

(6) Verantwortung für die Durchführung der Prüfung der organisatorisch-technischen Maßnahmen des Lieferanten nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG.

Zudem sind im Rahmen der vertraglichen Regelungen aus Transparenz- und Effizienzgründen Ansprechpartner zu benennen. Für den Datenschutz ist der DSB entsprechend aufzuführen.

DSB als Nutzer von ITSM-Tools

Eine weitere Beteiligungsform resultiert aus den zur Prozessunterstützung eingesetzten ITSM-Tools. Dort, wo Datenschutzbelange betroffen sind, sind diese auch in den verschiedenen Softwaretools abzubilden. In diesem Falle muss der DSB Zugriff auf die Tools haben, wobei seine Berechtigungen (Schreiben, Lesen etc.) unterschiedlich zu konzipieren sind. Im Rahmen des Lieferantenmanagements benötigt der DSB Zugriff auf die Supplier and Contract Database, die umfassende Informationen zu Lieferanten, Verträgen und den vom Lieferanten betriebenen Services enthält.[54] Mit Hilfe der SCD ist der DSB in der Lage, z. B. datenschutzrelevante Eintragungen oder Verträge zu prüfen und Reviewberichte einzusehen.

DSB als Prozessinitiator

Eng verknüpft mit der Wahrnehmung einer verantwortlichen Rolle im Lieferantenmanagement ist auch die Initiatorfunktion des DSB, die sich auf den Prozess insgesamt oder einzelne Aufgaben erstrecken kann. So hat er bei Vorliegen von Auftragsdatenverarbeitung sowohl die Prüfung der organisatorisch-technischen Maßnahmen des Lieferanten nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG als auch die Rückgabe überlassener Datenträger und die Lö-

[53] Vgl. *ITIL SD 2007*, S. 163.
[54] Vgl. *ebd.*

schung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags§ 11 Abs. 2 Satz 2 Nr. 10 BDSG zu initiieren.

Zusammenhänge

Mitunter sind die verschiedenen Formen der Beteiligung des DSB als Stakeholder miteinander verknüpft. So ist der Zugriff auf die Supplier and Contract Database Voraussetzung für die Stellungnahmen des Datenschutzbeauftragten. Eine umfangreichere Verantwortung hängt häufig mit dem Empfang von Informationen und einer Initiatorfunktion zusammen. Die Mitgliedschaft in verschiedenen Gremien bedeutet gleichzeitig, dass der DSB Adressat entsprechender Dokumentationen und Berichte ist. Auch wenn somit eine Trennung der Beteiligungsformen im Einzelfall schwierig ist, kann diese Systematik doch als Analyseraster helfen zu entscheiden, wo Möglichkeiten und Notwendigkeiten für die Integration des Datenschutzbeauftragten in einen ITIL-Prozess bestehen. Tabelle 6 zeigt ein solches Raster als exemplarische Stakeholder-Matrix aus Beteiligungsformen und Einzelaufgaben eines IT-Prozesses.

Tabelle 6
Stakeholder-Matrix für die Prozessintegration des DSB

	IT-Prozess		
Beteiligungsformen	Aufgabe 1	…	Aufgabe n
Stellungnahme			
Gremienmitgliedschaft			
Informationsempfänger			
Adressat von Berichten			
Verantwortungsträger			
Nutzer von ITSM-Tools			
Prozessinitiator			

4. Unternehmensindividuelle Analyse und Umsetzung

Situative Herangehensweise

Inwieweit Datenschutz in einem Unternehmen in die IT-Prozesse nach ITIL integriert wird, hängt weniger von den Anforderungen des Datenschutzes ab. Diese sind entsprechend der gesetzlichen Vorgaben grundsätzlich transparent, auch wenn es in der konkreten Umsetzung sicherlich Gestaltung- und Entscheidungsspielräume gibt. Ein ungleich wichtigerer situativer

Faktor ist der Grad der jeweiligen ITIL-Umsetzung.[55] Es war bereits erwähnt worden, dass in den Unternehmen der Umfang der realisierten ITIL-Prozesse durchaus variiert. Wohl kaum ein Unternehmen dürfte heute ITIL vollständig und „lupenrein“ umgesetzt haben. Insofern hängt es vom unternehmensindividuellen ITIL-Status ab, auf welche Weise der Datenschutz am besten zu integrieren ist. Somit ist eine unternehmensindividuelle Vorgehensweise erforderlich, vgl. Abbildung 9, wobei die ersten drei Schritte überwiegend überlappend und gegeneinander rückgekoppelt erfolgen sollten.

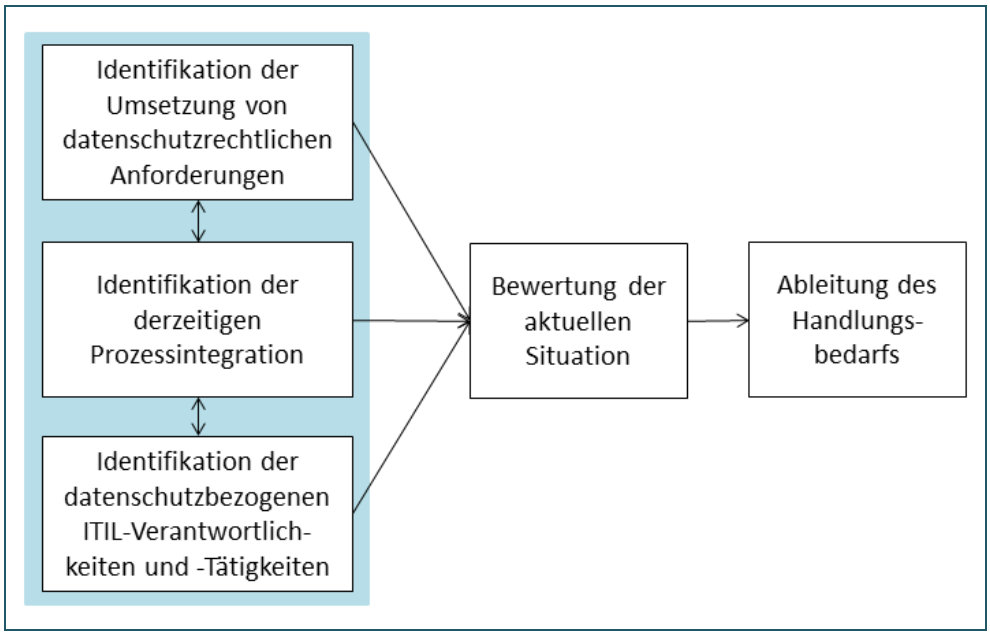

Abbildung 9
Vorgehen zur Integration des Datenschutzes in ITIL

(1) Identifikation der Umsetzung von datenschutzrechtlichen Anforderungen in den realisierten ITIL-Prozessen: Es ist in Bezug auf die vorhandenen ITIL-Prozesse zu prüfen, wo und wie gesetzliche Datenschutzanforderungen identifiziert und umgesetzt wurden (sollten die DS-Anforderungen an dieser Stelle nicht transparent sein, wäre hierfür eine entsprechende Analyse vorzuschalten).

(2) Identifikation der derzeitigen Prozessintegration des Datenschutzes in ITIL: Es ist zu analysieren, welche Formen der Prozessintegration des Datenschutzes aktuell realisiert sind, d. h. ist Datenschutz als Aufgaben-

[55] Weitere situative Faktoren wären etwa das unternehmensspezifische Verständnis des Datenschutzes, die im Unternehmen gelebte „Datenschutzkultur“ oder die Rolle und der Verantwortungsumfang des Datenschutzbeauftragten.

inhalt berücksichtigt, stellt Datenschutz eine Prozessanforderung dar und wo und wie finden sich Datenschutzaspekte in den verschiedenen eingesetzten ITSM-Tools wieder?

(3) Identifikation der datenschutzbezogenen ITIL-Verantwortlichkeiten und -Tätigkeiten: Hier ist danach zu fragen, welche Stakeholder derzeit in den ITIL-Prozessen eine datenschutzbezogene Verantwortlichkeit wahrnehmen. Hierbei ist insbesondere die aktuelle Einbeziehung des Datenschutzbeauftragten zu untersuchen.

(4) Bewertung der aktuellen Situation: Anhand der Analysen in diesen drei Bereichen kann nun eine Bewertung vorgenommen werden, inwieweit eine Integration des Datenschutzes in die derzeitigen IT-Prozesse nach ITIL erfolgt. Das Ergebnis für alle oder eben nur für die unternehmensrelevanten IT-Prozesse wird sich wie in Tabelle 7 schematisch gezeigt darstellen.

Tabelle 7
Bewertung der DS-Integration in die ITIL-Prozesse

ITIL-Prozesse	DS-Anforderungen	DSB-Integration	Prozessintegration
Service Catalogue Management	○	○	○
Service Level Management	○	●	○
Capacity Management	○	○	○
Availability Management	○	●	○
IT Service Continuity Management	○	○	●
Information Security Management	●	●	●
Supplier Management	●	●	○
		● hoch ● mittel ○ gering	

(5) Ableitung des Handlungsbedarfs: Auf Basis der Bewertung sind Maßnahmen festzulegen, die die Berücksichtigung des Datenschutzes und des Datenschutzbeauftragten in den IT-Prozessen nach ITIL stärken. Tabelle 8 zeigt beispielhaft sechs Maßnahmen für den Prozess „Supplier Management“. Diese Maßnahmen müssen selbstverständlich breit abgestimmt sein, insbesondere mit den jeweiligen Process-Owern und dem DSB.

Tabelle 8
Maßnahmen für den Prozess „Supplier Management“

ITIL-Prozess	Maßnahmen
…	
Supplier Management	(1) Es ist festzulegen, dass und welche datenschutzrechtlichen Vorgaben im Supplier Management relevant sind. (2) Die Beteiligung des DSB ist für den gesamten Prozess des Lieferantenmanagements festzulegen, insb. hinsichtlich vertraglicher Gestaltungen und Bewertungen. (3) Der DSB ist an der vorvertraglichen Risikoanalyse zu beteiligen. Diese hat sich auch auf relevante gesetzliche Vorgaben zu erstrecken. (4) Der DSB ist an den „service/supplier”-Review Meetings und den Vertragsreview-Meetings zu beteiligen. (5) Der Zugang des DSB zur SCD ist explizit festzuhalten. (6) Bei einer (absehbaren oder vorzeitigen) Vertragsbeendigung ist der DSB nachweislich zu beteiligen.
…	

Die Umsetzung der Maßnahmen ist zu verfolgen. Nach einer gewissen Umsetzungszeit ist der aktuelle Status je Maßnahme mit den betroffenen ITIL-Verantwortlichen zu klären. Die Struktur dieses Umsetzungscontrollings orientiert sich somit an den ITIL-Prozessen.

Literaturangaben

Bock 2010: Bock, Ingo: Optimierung von IT-Serviceorganisationen – Effizienz- und Qualitätssteigerung in der IT-Produktion, dpunkt, Heidelberg 2010.

Böttcher 2010: Böttcher, Roland: IT-Service-Management mit ITIL V3 – Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen, 2., akt. Aufl., Heise, Hannover 2010.

BSI 2005: Bundesamt für Sicherheit in der Informationstechnik: ITIL und Informationssicherheit – Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management, BSI, Bonn 2005, online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITIL/itil_pdf.pdf?__blob=publicationFile, Zugriff am 22.07.2012.

Dohle u. a. 2009: Dohle, Helge; Schmidt, Rainer; Zielke, Frank; Schürmann, Thomas: ISO 20000 – Eine Einführung für Manager und Projektleiter, dpunkt, Heidelberg 2009.

Dolle 2005: Dolle, Wilhelm: Incident Management. In: Datenschutz und Datensicherheit (DuD) , Nr. 7, 2005, S. 426, online verfügbar unter: http://www.dolle.net/paper/incident_management_dud05.pdf, Zugriff am 22.07.2012

Hoeren 2010: Hoeren, Thomas: Das neue BDSG und die Auftragsdatenverarbeitung. In: Datenschutz und Datensicherheit (DuD), Nr. 10, 2010, Jg. 34, S. 688-691.

Huber 2009: Huber, Bernhard M.: Managementsysteme für IT-Serviceorganisationen – Entwicklung und Umsetzung mit EFQM, COBIT, ISO 20000, ITIL, dpunkt, Heidelberg 2009.

ISACA 2011: ISACA Germany Chapter e.V. (Hg.): ISACA-Leitfaden zur Auftragsdatenverarbeitung unter Berücksichtigung von Standards, dpunkt, Heidelberg 2011.

ITGI 2011: IT-Governance Institute (ITGI): Global Status Report on the Governance of Enterprise IT (GEIT) – 2011, ITGI, Rolling Meadows 2011, online verfügbar unter: http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf, Zugriff am 22.07.2012.

ITIL SD 2007: Office of Government Commerce: ITIL – Service Design, The Stationery Office (TSO), London 2007.

ITIL SO 2007: Office of Government Commerce: ITIL – Service Operation, The Stationery Office (TSO), London 2007.

ITIL SS 2007: Office of Government Commerce: ITIL – Service Strategy, The Stationery Office (TSO), London 2007.

ITIL ST 2007: Office of Government Commerce: ITIL – Service Transition, The Stationery Office (TSO), London 2007.

Johannsen/Goeken 2011: Johannsen, Wolfgang; Goeken, Matthias: Referenzmodelle für IT-Governance – Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, 2. Aufl., dpunkt, Heidelberg 2011.

Klotz 2011: Klotz, Michael: IT-Compliance. In: Tiemeyer, Ernst (Hg.): Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 3. überarb. Aufl., Carl Hanser, München-Wien 2011, S. 585-639.

Köhler 2006: Köhler, Peter T.: ITIL: Das IT-Servicemanagement Framework, 2. Aufl., Springer, Berlin-Heidelberg 2006.

Materna 2010: Materna GmbH (Hg.): Executive Survey 2009: Status quo im IT Service Management, Ergebnisbericht, 2010.

Sowa 2008: Sowa, Aleksandra: IT-Sicherheit durch Zugriffs- und Zugangskontrollen. In: Hildebrand, K.; Meinhardt, S. (Hg.): Compliance & Risk Management. HMD Praxis der Wirtschaftsinformatik, Nr. 263, 2008, Jg. 45, S. 78-88.

Witt 2008: Witt, Bernhard C.: Datenschutz kompakt und verständlich – Eine praxisorientierte Einführung, Vieweg, Wiesbaden 2008.

Zarnekow/Brenner 2004: Zarnekow, Rüdiger, Brenner, Walter, Integriertes Informationsmanagement – Vom Plan, Build, Run zum Source, Make, Deliver. In: Zarnekow, R., Brenner, W., Grohmann, H. (Hrsg.): Informationsmanagement – Konzepte und Strategie für die Praxis, dpunkt, Heidelberg 2004, S. 3-24.

Firmenkurzprofil SERVIEW GmbH

Die SERVIEW GmbH mit Sitz in Bad Homburg ist eine spezialisierte Unternehmensberatung für IT Organisationen. SERVIEW wurde im Jahr 2002 gegründet und beschäftigt aktuell 55 festangestellte Mitarbeiter. Geschäftsführer sind Michael Kresse, Markus Bause und Kerstin Kresse. Als international agierendes Unternehmen optimiert SERVIEW die organisatorischen Fähigkeiten von IT Organisationen und unterstützt ihre Kunden bei deren Entwicklung zum Business Partner. Die Säulen der SERVIEW Dienstleistungen zum Etablieren von Business IT Alignement sind Beratung, Schulung und Events. Die methodische Basis für diese Dienstleistungen liefern Best Practice Frameworks und Standards wie ITIL®, PRINCE2®, ISO/IEC 20000®, COBIT®, M_o_R®, u.v.m.. Im Selbstverständnis der SERVIEW basiert eine nachhaltige und wertschöpfende Entwicklung der IT zum Business Partner auf Verständnis und Akzeptanz der Beteiligten und Betroffenen sowie dem Willen der Verantwortlichen. Neben der fachlichen und methodischen Expertise stehen das Herstellen und Aufrechterhalten dieser kritischen Erfolgsfaktoren im Fokus der Dienstleistungen von SERVIEW. Referenzkunden von SERVIEW sind unter anderem: VHV IS GmbH, TUI InfoTec GmbH, Merck KGaA, Krones AG, BG Phoenics GmbH.

Gründe für SERVIEW

SERVIEW verfügt über mehr festangestellte akkreditierte Trainer und Berater für ITIL®, PRINCE2®, MoR®, MSP®, P3O®, ISO20000 als jedes andere Unternehmen in Deutschland, Österreich und der Schweiz.

SERVIEW verfügt über mehr Akkreditierungen für Best Management Practice Methoden (wie z.B. ITIL®, PRINCE2® und MoR®) als jedes andere Unternehmen in Deutschland, Österreich und der Schweiz.

SERVIEW hat in Deutschland mehr IT-Organisationen erfolgreich zur ISO20000 Zertifizierung geführt als jedes andere Unternehmen.

SERVIEW hat in den letzten 10 Jahren mehr Teilnehmer in ITIL®, MoR®, PRINCE2®, MSP®, P3O® und ISO20000 in Deutschland, Österreich und der Schweiz ausgebildet als jedes andere Beratungs- unternehmen.

SERVIEW bildet pro Jahr mehr Schulungsteilnehmer in ITIL®, PRINCE2®, MoR®, MSP®, P3O® und ISO20000 in Deutschland, Österreich und der Schweiz aus als jedes andere Beratungsunternehmen.

SERVIEW ist der Erfinder und Rechteinhaber des Workbook-Prinzips® für Best Management Practice Seminare. Kein anderes Schulungskonzept

wurde von anderen ITIL® Schulungsanbietern so oft kopiert, wie das SERVIEW Workbook-Prinzip.

SERVIEW investiert wie kein anderes Beratungsunternehmen in Europa so viel Aufwand in die Durchführung von PowerPoint-freien Seminaren.

SERVIEW bietet wie kein anderes Unternehmen im Jahr so viele Schulungen mit Termin-Garantie für ITIL®, PRINCE2®, MSP®, MoR®, P3O® an.

SERVIEW ist das erste akkreditierte Unternehmen in Deutschland für die PRINCE2® Professional Zertifizierung.

SERVIEW ist das einzige Unternehmen in Deutschland, in dem ausschließlich eigene festangestellte Trainer für alle Best Management Practice Methoden Seminare wie ITIL®, PRINCE2®, MoR®, MSP®, P3O® eingesetzt werden.

SERVIEW fokussiert wie kein anderes Beratungsunternehmen in Deutschland sich so konsequent auf die Best Management Practice Methoden wie ITIL®, PRINCE2®, MoR®, MSP® und P3O®.

SERVIEW veröffentlich seit 10 Jahren mehr ITIL® Fachbücher als jedes andere deutsche Beratungshaus.

SERVIEW hat die erfolgreichste deutschsprachige Fach-App (Apple) für ITIL® v3 veröffentlicht.

SERVIEW ist der Erfinder der erfolgreichsten ITIL®, PRINCE2®, MSP®, P3O®, MoR® Intensiv Seminare in Europa.

SERVIEW führt wie kein anderes Unternehmen in Europa so viele ITIL®, PRINCE2®, MSP®, P3O®, MoR® Intensiv Seminare.

SERVIEW veranstaltet den größten Anwenderkongress für Best Management Practice Methoden in Deutschland.

SERVIEW ist das weltweit erste und einzige Beratungsunternehmen mit einem unabhängig bescheinigten (DQS) ISO 20000 konformen Beratungsansatz.

SERVIEW hat die weltweit erste und erfolgreichste ITIL® Hör-Inszenierung veröffentlicht.

SERVIEW ist Vorsprung erleben!

Webseite: http://www.serview.de/
Ansprechpartner Marketing & PR: Kerstin Dorn

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf

wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu werden Labore als Demonstrationsbereiche unterhalten. In den Laboren werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de
🌍 www.simat.fh-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Kaminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesund-heitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutschsprachige Museums-Apps
03-11-016	11.2011	S. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Meck-lenburg-Vorpommern – Strom als Wettbewerbs-faktor und Gegenstand der Standortvermarktung
04-12-017	04.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL