ZIK

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

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Datenschutz-Managementsysteme im Aufwind?

Schulthess §

62

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

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Datenschutz-Managementsysteme im Aufwind?

Schulthess § 2016

62

Das 1998 geschaffene «Zentrum für Informations- und Kommunikationsrecht» an der Rechtswissenschaftlichen Fakultät der Universität Zürich (Lehrstuhl Prof. Dr. Rolf H. Weber, Rämistrasse 74, 8001 Zürich) dient als Forschungsstelle sowie als Anlauf- und Kontaktstelle für an diesem Rechtsgebiet interessierte Personen und Gruppen.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7255-7469-8

www.schulthess.com

Inhaltsverzeichnis

MARIA WINKLER*

Implementierung, Auditierung und Zertifizierung von Datenschutz-Managementsystemen

Inhaltsverzeichnis

* MARIA WINKLER, mag. iur., ist als Rechtsberaterin im Bereich IT-Recht sowie als Auditorin für Datenschutz-Managementsysteme im Auftrag der SQS tätig.

I. Einleitung

Die in den letzten Jahren vermehrt stattfindende öffentliche Berichterstattung über Datenschutzthemen führte unter anderem auch dazu, dass sich Unternehmen vermehrt die Frage stellen, welche vorsorglichen Massnahmen sie zur Verhinderung von Datenschutzverletzungen ergreifen müssen. Auch wenn ein Verstoss gegen das Datenschutzgesetz bis heute kaum schwerwiegende rechtliche Folgen nach sich zieht, besteht zumindest das Risiko von negativer Berichterstattung in den Medien, was die Unternehmen wegen des damit verbundenen Image- und Vertrauensverlusts verhindern wollen. Aus diesem Grund ernennen viele Unternehmen auch ohne eine diesbezügliche gesetzliche Verpflichtung Datenschutzbeauftragte, die für Fragen des Datenschutzes und der Datensicherheit verantwortlich sind und die entsprechende Massnahmen im Unternehmen umsetzen.

Um nachweisen zu können, dass die eigenen Datenbearbeitungsverfahren gesetzeskonform sind, entscheiden sich auch immer mehr Unternehmen freiwillig für eine Datenschutzzertifizierung. Die Normen, welche dabei eingehalten werden müssen, geben eine Anleitung für den Aufbau eines Datenschutz-Managementsystems (DSMS), bei deren Einhaltung der Nachweis der Beachtung der eigenen Sorgfaltspflichten erleichtert wird. Zudem kann ein Datenschutzzertifikat als Marketinginstrument in der Kommunikation mit Kunden genutzt werden.

Der Aufwand, der für eine erfolgreiche Datenschutzzertifizierung erforderlich ist, wird nicht selten unterschätzt. Für den Erwerb eines Datenschutzzertifikats reicht es nicht aus, sicherzustellen, dass die Datenbearbeitungen im Unternehmen gesetzeskonform erfolgen. Für eine Datenschutzzertifizierung muss ein DSMS aufgebaut werden, das für eine systematische Einhaltung des Datenschutzes im Unternehmen geeignet sein muss. Setzt sich das Unternehmen nicht rechtzeitig mit den Normanforderungen an ein DSMS auseinander, besteht das Risiko, dass der zeitliche und finanzielle Aufwand für die Datenschutzzertifizierung unterschätzt und im schlimmsten Fall das Zertifikat nicht erreicht wird.

Das vorliegende Kapitel gibt eine einführende Übersicht über die verschiedenen Datenschutzzertifizierungen in der Schweiz und im umliegenden Ausland und geht anschliessend auf die Anforderungen einer erfolgreichen Datenschutzzertifizierung nach der VDSZ ein. Die folgenden Ausführungen enthalten keine umfassende Anleitung für den Aufbau eines DSMS, sondern

sie konzentrieren sich auf Normanforderungen, deren Umsetzung in der Praxis häufig Probleme verursachen und geben Tipps, wie diese vermieden werden können.

II. Datenschutzzertifizierungen in der Schweiz und im Ausland

1. Schweiz

Mit der Teilrevision des DSG wurde die Möglichkeit einer Datenschutzzertifizierung als Instrument der Selbstregulierung in Art. 11 DSG eingefügt. Hersteller von Datenbearbeitungssystemen oder –programmen sowie private Personen und Bundesorgane, die Personendaten bearbeiten, können nach dieser Bestimmung ihre Systeme, Verfahren und ihre Organisation durch unabhängige Zertifizierungsstellen prüfen und zertifizieren lassen. Von der Freiwilligkeit der Datenschutzzertifizierung besteht seit dem 01. Januar 2013 eine Ausnahme. Krankenversicherer müssen für den Empfang von Fallpauschalenrechnungen nach dem Tarifsystem SwissDRG über eine nach Art. 11 DSG zertifizierte Datenannahmestelle verfügen[1].

Die Datenschutzzertifizierungen nach Art. 11 DSG sind in der VDSZ geregelt. Sie sieht die Zertifizierung von Organisation und Verfahren (DSMS-Zertifizierung[2]) sowie die Zertifizierung von Produkten (Produktzertifizierung[3]) vor. Allerdings wurde die Zertifizierung von Produkten durch den EDÖB nach einer Prüfung im Rahmen einer Arbeitsgruppe einstweilen eingefroren, da diese als nicht sinnvoll erachtet wurde[4]. Derzeit ist es somit nur möglich, Organisation und Verfahren (sogenannte DSMS) nach VDSZ zu zertifizieren. Unternehmen, die die erfolgreiche Zertifizierung dem EDÖB melden, sind von ihrer Meldepflicht für diejenigen Datensammlungen befreit[5], welche im Zertifizierungsumfang enthalten sind (siehe dazu die Ausführungen zum Geltungsbereich der Zertifizierung in Abschnitt III). Der

---

1 Art. 59a Abs. 6 KVV.
2 Art. 4 VDSZ.
3 Art. 5 VDSZ.
4 http://www.edoeb.admin.ch/datenschutz/00756/00757/index.html?lang=de, besucht am 25.12.2015.
5 Art. 11a Abs. 5 Bst. f DSG.

EDÖB führt auf seiner Website eine Liste mit den Unternehmen, welche sich durch die Meldung einer VDSZ-Zertifizierung von ihrer Meldepflicht für Datensammlungen befreit haben[6]. Die Meldung einer VDSZ-Zertifizierung beim EDÖB verpflichtet das zertifizierte Unternehmen aber auch, allfällige im Rahmen eines Audits durch die Zertifizierungsstelle festgestellte Schwachstellen dem EDÖB zu melden[7]. Da die Befreiung von der Meldepflicht auch durch die Mitteilung der Ernennung eines betrieblichen Datenschutzverantwortlichen[8] erfolgen kann, verzichten viele zertifizierte Unternehmen auf die Meldung der Zertifizierung. Daher ist die Anzahl der nach VDSZ zertifizierten Unternehmen bei weitem grösser als es nach der Liste des EDÖB den Anschein macht.

Neben einer Zertifizierung nach VDSZ besteht auch die Möglichkeit einer Zertifizierung nach dem Schweizer Label GoodPriv@cy. Dabei handelt es sich um eine geschützte Garantiemarke, welche durch eine private Trägerschaft gehalten wird[9]. Im Gegensatz zur Zertifizierung nach der VDSZ befreit der Erwerb des Labels GoodPriv@cy nicht von der Meldepflicht für Datensammlungen. Zertifizierungen nach GoodPriv@cy findet man vielfach ausserhalb des Anwendungsbereichs des DSG und auch im Ausland.

Da sich sowohl die VDSZ als auch das Label GoodPriv@cy eng an ISO-Normen anlehnen, sind sie inhaltlich sehr ähnlich. Daher entscheiden sich Unternehmen nicht selten dafür, sich nach beiden Normen zertifizieren zu lassen.

2. Ausland

Der Blick ins umliegende Ausland zeigt, dass Datenschutzzertifizierungen in einigen der umliegenden Staaten zwar gesetzlich vorgesehen sind, die Umsetzung in der Praxis aber vielfach noch nicht oder noch nicht vollständig erfolgt ist. Im Folgenden wird ein kurzer Überblick über die Datenschutzzertifizierungen in der Europäischen Union, in Deutschland und in Liechtenstein gegeben.

---

6 http://www.edoeb.admin.ch/datenschutz/00756/index.html?lang=de, besucht am 31.12.2015.

7 Art. 8 Abs. 2 VDSZ.

8 Art. 11 a Abs. 5 Bst. e DSG.

9 http://www.sqs.ch/de/Leistungsangebot/Produkte/Labels/GoodPriv@cy/L.GPR, besucht am 25.12.2015.

Die neue Datenschutz-Grundverordnung der EU (DSGV) sieht die Förderung von freiwilligen Datenschutzzertifizierungen durch die Mitgliedsstaaten und durch die Kommission auf europäischer Ebene vor[10]. Die Kommission wird ermächtigt, entsprechende delegierte Rechtsakte zu erlassen. Mit Inkrafttreten der DSGV wird daher der Grundstein für einen einheitlichen Rechtsrahmen für Datenschutzzertifizierungen in der EU gelegt werden.

Mit dem Europäischen Datenschutzgütesiegel EuroPriSe[11] können IT-Produkte und IT-basierte Dienstleistungen zertifiziert werden. Bei EuroPriSe handelt es sich um eine Initiative des Unabhängigen Landeszentrums für Datenschutz des deutschen Bundeslands Schleswig Holstein (ULD), an dem acht weitere Partner beteiligt sind und die von der Europäischen Union gefördert wird[12].

In Deutschland sieht §9a des Bundesdatenschutzgesetzes (BDSG, BGBl I S. 2355) Regeln zum Datenschutzaudit vor. Allerdings fehlt das für die Umsetzung erforderliche Ausführungsgesetz[13]. Im deutschen Bundesland Schleswig Holstein sieht das Landesdatenschutzgesetz (LDSG) vor, dass öffentliche Stellen ein Datenschutzaudit durch das Unabhängige Landeszentrum für Datenschutz (ULD) beantragen können[14]. Gemäss der auf der Website des ULD aufgeschalteten Liste der zertifizierten Behörden wurde diese Möglich-

---

10 Art. 39 der DSGV in der Fassung des konsolidierten Texts vom 15.12.2015, abrufbar unter http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf, besucht am 29.12.2015.

11 Nähere Informationen findet man auf der Website von EuroPriSe unter https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe, besucht am 29.12.2015.

12 Vgl. dazu GLOOR SCHEIDEGGER, Datenschutz-Zertifizierung, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, Rz 23.21.

13 Siehe dazu die Ausführungen zum Datenschutzaudit auf der Website der Bundesbeauftragten für den Datenschutz und die Informationssicherheit unter http://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/Datenschutzaudit.html?nn=5217238, besucht am 29.12.2015.

14 Nähere Informationen zum Datenschutz-Behördenaudit des ULD findet man auf der Website des ULD unter https://www.datenschutzzentrum.de/audit/, besucht am 02.01.2016.

keit der freiwilligen Zertifizierung bereits von zahlreichen Behörden genutzt[15].

In Liechtenstein sieht das Datenschutzgesetz eine Zertifizierung von Produkten, Systemen, Verfahren sowie der Organisation von Herstellern von Datenbearbeitungssystemen oder –programmen sowie von Privaten oder Behörden, die Personendaten bearbeiten, vor[16]. Im Gegensatz zur Schweiz ist in Liechtenstein auch eine Zertifizierung von Produkten möglich und es wurde ein offizielles Datenschutz-Qualitätszeichen (Gütesiegel) entwickelt, das zertifizierte Unternehmen zur Kennzeichnung ihrer zertifizierten Produkte, Systeme, Verfahren und Organisationen verwenden können. Zertifizierungsstellen, die Datenschutzzertifizierungen nach Art. 14a DSG FL durchführen, müssen bei der Liechtensteiner Akkreditierungsstelle akkreditiert sein[17]. Gemäss dem Verzeichnis der akkreditierten Stellen, das auf der Website der Liechtensteiner Akkreditierungsstelle abrufbar ist, ist bis heute aber keine Zertifizierungsstelle nach VDSZ FL akkreditiert[18].

III. Der Weg zum Datenschutzzertifikat nach VDSZ

1. Vorbemerkung

Je nachdem, wie die Organisation aufgebaut ist, welche Datenbearbeitungen stattfinden und was genau Gegenstand der Zertifizierung ist, werden von der Einführung eines DSMS alle oder zumindest ein Grossteil der Mitarbeitenden auf die eine oder andere Weise in ihrer Arbeit betroffen sein. Die Personen, welche den Zertifizierungsprozess im Unternehmen planen und leiten (häufig handelt es sich dabei um Datenschutzbeauftragte, Datensicherheitsbeauftragte oder Qualitätsbeauftragte), müssen dabei sowohl auf die interne Mitwirkung der betroffenen Mitarbeitenden zählen als auch, falls notwendig, externe Unterstützung beiziehen oder allenfalls Schulungen besuchen können.

---

15 https://www.datenschutzzentrum.de/audit/register/, besucht am 02.01.2016.
16 Art. 14a DSG FL; LR-Nr. 235.1.
17 Art. 2 Abs. 1 VDSZ FL; LR-Nr. 235.111.
18 http://www.llv.li/files/avw/7354-akkreditierte-stellen-li-v20150331-nath-sig.pdf, besucht am 31.12.2015.

Aus den genannten Gründen sollte die Entscheidung, ein Datenschutzzertifikat zu erwerben, durch die Unternehmensführung getroffen oder durch diese zumindest ausdrücklich unterstützt werden. Nur so kann gewährleistet werden, dass die erforderlichen personellen und finanziellen Ressourcen bereitgestellt werden und allenfalls nötige Anpassungen von bestehenden unternehmensinternen Abläufen umgesetzt werden können.

Um die für die Unterstützung des Managements erforderlichen Informationen aufzubereiten, müssen daher bereits im Rahmen der Vorbereitung der Zertifizierung erste Schritte unternommen werden, die es dem Unternehmen ermöglichen, den für das Erreichen einer Datenschutzzertifizierung erforderlichen Aufwand sowie die Auswirkungen auf die unternehmensinternen Prozesse abzuschätzen. Im Folgenden werden einige Massnahmen und Tätigkeiten erläutert, die möglichst frühzeitig ergriffen werden sollten.

2. Studium der VDSZ

Die VDSZ besagt nicht nur, welche Dokumente und Prozesse für die Zertifizierung des DSMS vorhanden sein müssen sondern sie gibt vielfach auch vor, welchen Anforderungen der Inhalt von Dokumenten entsprechen muss. Nur bei genauer Kenntnis der Norm kann daher Klarheit darüber gewonnen werden, welche Elemente eines DSMS im Unternehmen allenfalls bereits vorhanden sind und welche Normanforderungen neu umgesetzt werden müssen. Daher ist es unerlässlich, sich mit den Anforderungen der VDSZ an ein DSMS frühzeitig auseinanderzusetzen. Die VDSZ und die durch den EDÖB publizierten ergänzenden Dokumente basieren auf internationalen Normen, deren Inhalte aus urheberrechtlichen Gründen nicht direkt sondern mittels Verweisen übernommen wurden und die daher ebenfalls konsultiert werden müssen. Unternehmen, die bereits nach ISO 9001 oder nach ISO/IEC 27001:2013 zertifiziert sind, haben in der Regel einen bedeutend geringeren Aufwand für den Aufbau eines DSMS, da die Anforderungen der VDSZ sich in einem wesentlichen Teil mit denen der genannten Normen decken.

Ein DSMS umfasst die Datenschutzpolitik, die Dokumentation von Zielen und Massnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit sowie die organisatorischen und technischen Vorkehrungen zur

Verwirklichung der festgelegten Ziele und Massnahmen, insbesondere die Vorkehrungen zur Behebung festgestellter Mängel[19].

Die Mindestanforderungen, die das DSMS erfüllen muss, sind in den Zertifizierungsrichtlinien des EDÖB festgelegt[20]. Diese verweisen auf die Norm ISO/IEC 27001:2013, auf deren Basis Informationssicherheits-Managementsysteme zertifiziert werden. Dabei müssen an den Vorgaben der ISO/IEC 27001:2013 an ein ISMS für ein DSMS gewisse Anpassungen gemacht werden. So ist der Begriff der Informationssicherheit durch den Begriff Datenschutz zu ersetzen[21] und das Risikomanagement muss für den Bereich Datenschutz durch das sogenannte Konformitätsmanagement ergänzt werden. Das Vorgehen des EDÖB basiert auf der Vorgabe von Art. 4 Abs. 3 VDSZ, wonach beim Erlass der Zertifizierungsrichtlinien internationale Normen zu berücksichtigen sind. Sie führen aber dazu, dass für die Kenntnis der genauen Anforderungen an ein DSMS nach VDSZ die Norm ISO/IEC 27001:2013 käuflich erworben werden muss, da diese urheberrechtlich geschützt sind.

Die Zertifizierungsrichtlinien enthalten in Ziffer 5 die verschiedenen Ziele und Massnahmen, welche bei der Erstellung des DSMS erfüllt sein müssen. Dabei handelt es sich um die Datenschutzgrundsätze des DSG, die wiederum im Leitfaden für das Datenschutz-Management (im Folgenden Leitfaden) genauer erläutert werden[22]. Zudem gibt es auf der Website des EDÖB noch Erläuterungen zu den Zertifizierungsrichtlinien sowie weitere Dokumente, welche das Verständnis der Anforderungen der VDSZ erleichtern sollen. Aufgrund des Inkrafttretens der revidierten Version der ISO/IEC 27001:2013 wurden zudem die Zertifizierungsrichtlinien sowie die Erläuterungen angepasst. Die neuen Erläuterungen von 2014 enthalten nur Erklärungen über die Anpassungen und verweisen sonst auf die Erläuterungen von 2008, weshalb diese immer noch zusätzlich mitberücksichtigt werden müssen.

Insgesamt handelt es sich somit um ein komplexes System von Dokumenten, in welchen die Anforderungen an ein DSMS nach VDSZ abgebildet sind. Al-

---

19 Art. 4 Abs. 2 VDSZ.

20 http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html, besucht am 27.12.2015.

21 Ziffer 3 Abs. 2 Zertifizierungsrichtlinien 2014.

22 Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, abrufbar unter http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html, besucht am 27.12.2015.

le mit Ausnahmen der ISO/IEC 27001:2013 sind auf der Website des EDÖB abrufbar[23]. Erschwerend kommt hinzu, dass der EDÖB unterschiedliche Bezeichnungen der Dokumente verwendet. Im Folgenden sind die Dokumente, welche für eine Datenschutzzertifizierung zusätzlich zur VDSZ zwingend konsultiert werden müssen, aufgelistet[24]:

- Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren), vom 19. März 2014, publiziert auf der Website des EDÖB unter „Zertifizierungsrichtlinien 2014"
- Leitfaden für das Datenschutz-Management vom 15.04.2014, publiziert auf der Website des EDÖB unter „Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS 2014"
- Erläuterungen zu den Änderungen vom 19. März 2014 der „Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem" vom 15.04.2014, publiziert auf der Website des EDÖB unter „Erläuterungen zu den Richtlinien 2014"
- Erläuterungen zu den „Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem" vom 22.08.2008, publiziert auf der Website des EDÖB unter „Erläuterungen zu den Richtlinien 2008
- ISO/IEC 27001:2013.

Der genaue Inhalt und die Auswirkungen dieser Anforderungen auf das eigene Unternehmen sind in der Regel nicht ohne weitere Informationen verständlich. Daher ist es empfehlenswert, vor dem Aufbau eines DSMS entsprechende auf dem Markt erhältliche Schulungsangebote zu nutzen oder allenfalls externe Hilfe in Anspruch zu nehmen. So können Mängel bei der Zertifizierung vermieden werden. Einige Normanforderungen, deren Umsetzung in der Praxis häufig zu Problemen führen, werden in Abschnitt IV dieses Kapitels erläutert.

---

[23] http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html, besucht am 02.01.2016.

[24] Zusätzlich finden sich auf der Website des EDÖB unter http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html noch weitere Dokumente mit Erklärungen zu einzelnen Themen.

3. Auswahl der Zertifizierungsstelle

Eine Zertifizierung nach VDSZ kann nur durch Zertifizierungsstellen durchgeführt werden, welche nach der Akkreditierungs- und Bezeichnungsverordnung[25] akkreditiert sind. Die Akkreditierung beinhaltet die Prüfung und Anerkennung der fachlichen und organisatorischen Kompetenz der Zertifizierungsstellen und erfolgt durch die Schweizerische Akkreditierungsstelle SAS, die dafür den EDÖB beizieht[26]. Die akkreditierten Zertifizierungsstellen werden auf der Website der SAS publiziert[27]. Um akkreditiert zu werden, muss die Zertifizierungsstelle über eine festgelegte Organisation sowie über ein festgelegtes Zertifizierungsverfahren verfügen[28] und das Personal, welches die Datenschutzzertifizierungen durchführt, muss Kenntnisse in den Bereichen des Datenschutzrechts und der Informationssicherheit sowie eine Auditorenausbildung für Managementsysteme aufweisen[29]. Zurzeit sind zwei Unternehmen als Zertifizierungsstellen für Datenschutzzertifizierungen nach VDSZ akkreditiert[30].

Mit der Zertifizierungsstelle können die Kosten der Zertifizierung geklärt sowie das Vorgehen geplant werden. Der finanzielle Aufwand mit dem das Unternehmen für eine Datenschutzzertifizierung rechnen muss, setzt sich aber nicht nur aus den Kosten der Zertifizierung selbst zusammen. Der eigene interne aber auch der allenfalls erforderliche externe Unterstützungsaufwand sollte daher von Beginn an mit berücksichtigt werden. Die Kosten, die für eine Datenschutzzertifizierung insgesamt anfallen, sind je nach Unternehmen sehr unterschiedlich und werden vor allem beeinflusst vom Umfang der Zertifizierung (siehe dazu den folgenden Abschnitt), dem allenfalls im Unternehmen vorhandenen Know-how betreffend Management-Systemen, den bereits erstellten Reglementen und Weisungen sowie Prozessdokumentationen.

---

25 AkkB; SR 976.512.

26 Art. 2 VDSZ; für weitere Informationen siehe GLOOR SCHEIDEGGER (Fn. 12), Rz 23.26 f.

27 http://www.seco.admin.ch/sas/akkreditiertestellen/index.html?lang=de&, besucht am 25.12.2015.

28 Art. 1 Abs. 3 VDSZ.

29 Anhang zur VDSZ (Art. 1 Abs. 5): Mindestanforderungen an die Qualifikation des Personals der Zertifizierungsstellen, welches Zertifizierungen durchführt.

30 Es handelt sich um die Schweizerische Vereinigung für Qualitäts- und Managementsysteme SQS und die KPMG AG.

Die Zertifizierungsstellen selbst sind für die Prüfung und Zertifizierung des DSMS verantwortlich. Die Beratung für die korrekte Umsetzung der Normvorgaben gehört hingegen, zur Wahrung ihrer Unabhängigkeit, nicht zu den Aufgaben der Zertifizierungsstelle. Das entsprechende Wissen muss sich das Unternehmen daher selbst oder bei Dritten beschaffen.

4. Festlegung des Geltungsbereichs des Datenschutz-Managementsystems

Der detaillierten und vollständigen Beschreibung des Geltungsbereichs des DSMS kommt in der Praxis grosse Bedeutung zu. Dieser bestimmt, welche Datenbearbeitungen zertifiziert werden und legt somit den Umfang des DSMS und den genauen Gegenstand der Prüfung durch die Zertifizierungsstelle fest.

Den Unternehmen steht es grundsätzlich frei, den Umfang der Zertifizierung selbst festzulegen. Zertifizierbar sind entweder alle oder einzelne, abgegrenzte Datenbearbeitungsverfahren, für die das Unternehmen verantwortlich ist[31]. Es ist daher möglich und zulässig, nur den Personalprozess, oder einen Datenbearbeitungsprozess zu zertifizieren, mit dem besonders heikle Kundendaten bearbeitet werden, wie beispielsweise die Archivierung und / oder Vernichtung von Kundendaten. Ein weiteres Beispiel für die Zertifizierung eines einzelnen Datenbearbeitungsverfahrens ist die bereits erwähnte Zertifizierung der Datenannahmestelle für SwissDRG-Rechnungen bei Krankenversicherern (siehe dazu oben Abschnitt II Ziffer 1)[32].

Bei den Überlegungen, welche Datenbearbeitungen zertifiziert werden sollen, ist zu berücksichtigen, dass es in der Praxis häufig schwierig ist, einige zwingende Elemente eines DSMS (wie beispielsweise eine Datenschutzpolitik oder die Massnahmen zur Gewährleistung von Datenschutz und Datensi-

---

[31] Art. 4 Abs. 1 VDSZ.

[32] Der gesetzlich definierte Aufgabenbereich der Datenannahmestelle (und somit der Bereich, der gemäss Art. 59a KVV zwingend zertifiziert werden muss) umfasst den Eingang von DRG-Rechnungen, die sogenannte Dunkelprüfung auf der Basis von vordefinierten Prüfkriterien sowie die Auslenkung von auffälligen DRG-Rechnungen an den Versicherer zur weiteren Prüfung und die Weiterleitung von unauffälligen Rechnungen zur Bezahlung. Die weitere Prüfung der ausgelenkten auffälligen DRG-Rechnungen ist nicht mehr Aufgabe der Datenannahmestelle und muss daher nicht mehr geprüft und zertifiziert werden.

cherheit) nur für einzelne Datenbearbeitungsverfahren zu erstellen. Dies führt dazu, dass bei einer Zertifizierung nur eines oder einiger weniger Datenbearbeitungsverfahren teilweise nur ein unwesentlich geringerer Aufwand für die Erstellung des DSMS entsteht. Zudem lassen sich Abgrenzungsprobleme bei der Planung und Durchführung der Audits oft kaum vermeiden. Auch wenn alle Datenbearbeitungsverfahren zertifiziert werden, müssen diese in der Beschreibung des Geltungsbereichs des DSMS genügend genau bestimmt werden. Nur so kann sichergestellt werden, dass diese im Zertifizierungsaudit auch geprüft werden. Denn was der Zertifizierungsstelle beim Audit nicht vorliegt, kann diese nicht prüfen und ist daher auch nicht zertifiziert.

In die Beschreibung des Geltungsbereichs des DSMS müssen alle Informationen aufgenommen werden, die für die Prüfung der zu zertifizierenden Datenbearbeitungsverfahren wichtig sind. Dazu zählen

- die Bezeichnung der Datenbearbeitungsverfahren
- die Auflistung der relevanten Datensammlungen,
- der betroffenen Organisationseinheiten,
- der Standorte, an denen die Datenbearbeitungen erfolgen und
- der technischen Infrastruktur, die dabei eingesetzt wird.

Werden Datenbearbeitungsverfahren, die zertifiziert werden sollen, ganz oder teilweise an ein Drittunternehmen geoutsourct, dann muss dieser Umstand ebenfalls in die Beschreibung des Geltungsbereichs des DSMS aufgenommen und die Outsourcingpartner müssen benannt werden. Dies hat in der Regel zur Folge, dass die Zertifizierungsstelle auch die Datenbearbeitungen beim Outsourcingpartner vor Ort prüft. Eine Ausnahme ist möglich, falls der Outsourcingpartner selbst über eine entsprechende Zertifizierung der an ihn geoutsourcten Datenbearbeitung verfügt. Es lohnt sich daher, im Rahmen der Vorbereitung für eine Datenschutzzertifizierung eine Liste der betroffenen Outsourcingpartner zu erstellen und zu prüfen, ob diese selbst bereits über eine Zertifizierung der an sie geoutsourcten Datenbearbeitungsverfahren verfügen. In diesem Fall müssen der Zertifizierungsstelle allenfalls entsprechende Dokumente wie Berichte oder Zertifikate des Outsourcingpartners herausgegeben werden. Es liegt in der Verantwortung des Unternehmens, durch entsprechende vertragliche Vereinbarungen sicherzustellen, dass ein Audit der Datenbearbeitungsverfahren beim Outsourcingpartner durch die Zertifizierungsstelle möglich ist bzw. dass dieser verpflichtet ist, alle erforderlichen Informationen herauszugeben. Ist es der Zertifizierungsstelle nicht möglich,

den Outsourcingpartner zu prüfen oder Einsicht in die dafür allenfalls erforderlichen Berichte zu nehmen, führt dies in der Regel zu einer Nicht-Konformität auf Seiten des Unternehmens und im schlimmsten Fall zu einem Nicht-Bestehen des Zertifizierungsaudits. Es ist nicht Aufgabe der Zertifizierungsstelle, sich diese Informationen beim Outsourcingpartner des Unternehmens zu beschaffen.

Ist die Beschreibung des Geltungsbereichs des DSMS falsch oder unvollständig, dann besteht das Risiko, dass nicht alle Datenbearbeitungen vom Geltungsbereich des Zertifikats erfasst sind. Werden diese Lücken erst im Verlauf des Audits bemerkt, dann werden diese als Abweichungen von der Norm erfasst und führen entweder zu einem Nicht-Bestehen des Zertifizierungsaudits (man spricht in einem solchen Fall von einer sogenannten Major-Non-Conformity oder zertifikatsverhindernden Abweichung von der Norm) oder zu einer Auflage, unter der das Zertifikat erteilt wird (sogenannte Minor-Non-Conformity). In jedem Fall müssen die bisher nicht dokumentierten Elemente des DSMS nachträglich geprüft werden, was zusätzlichen Aufwand und zusätzliche Kosten verursacht. Es lohnt sich daher, genügend Zeit in die Beschreibung des Geltungsbereichs des DSMS zu investieren und diese bei allfälligen Änderungen zu aktualisieren.

IV. Aufbau und Implementierung eines Datenschutz-Managementsystems

1. Vorbemerkung

Gegenstand der Zertifizierung ist ein DSMS, somit ein Managementsystem, das die systematische Sicherstellung von Datenschutz und Datensicherheit im zertifizierten Bereich gewährleistet. Die ISO/IEC 27001:2013 und somit auch die VDSZ basieren auf dem sogenannten Planungskreislauf oder PDCA-Ansatz (Plan-Do-Check-Act). Ziel ist es, das Konformitätsniveau des DSMS während des Zertifizierungszyklus von 3 Jahren ständig zu verbessern oder zumindest aufrecht zu erhalten[33]. Dies bedingt, dass Verfahren festgelegt werden, um das DSMS regelmässig zu prüfen, zu aktualisieren und

[33] Erläuterungen des EDÖB zum Zertifizierungszyklus, abrufbar unter http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html, besucht am 30.12.2015.

wenn nötig zu ergänzen oder zu korrigieren. Zudem müssen die entsprechenden Aufgaben und Verantwortlichkeiten definiert und festgelegt werden. Nach dem Aufbau des DSMS und der erfolgreichen Zertifizierung folgen daher der Betrieb und die Verbesserung des DSMS als Daueraufgabe.

Die Elemente eines DSMS werden in den anderen Kapiteln dieses Buches detaillierter erläutert, daher wird an dieser Stelle auf eine umfassende Darstellung eines DSMS verzichtet. Die folgenden Abschnitte konzentrieren sich auf einzelne Aspekte eines DSMS, welche für die Unternehmen in der Praxis oft schwierig umzusetzen sind oder denen oft fälschlicherweise eine zu geringe Bedeutung beigemessen wird.

2. Dokumentation

Mit dem Aufbau und dem Betrieb eines DSMS ist ein Dokumentationsaufwand verbunden, der in der Praxis nicht genau abgeschätzt werden kann und daher zu Fehlkalkulationen führt. Die Dokumentation dient dem Nachweis, dass die festgelegten Massnahmen und Ziele des DSMS systematisch umgesetzt werden und auf einen Datenschutz- oder Datensicherheitsvorfall nicht nur situativ reagiert wird. Damit ein DSMS von der Zertifizierungsstelle geprüft werden kann, müssen daher Nachweise erstellt werden, welche die Systematik belegen.

Pauschal ausgedrückt reicht es für eine Datenschutzzertifizierung nicht aus, Datenschutz und Datensicherheit systematisch zu gewährleisten sondern dies muss auch durch die entsprechenden dokumentierten Nachweise belegt werden. Den betroffenen Unternehmen ist dabei meist klar, dass beispielsweise eine Datenschutzpolitik oder Weisungen im Bereich Datenschutz und Datensicherheit schriftlich und dokumentiert erstellt werden müssen (man bezeichnet diese als Vorgabedokumente oder Vorgabedokumentation). Anders ist dies aber häufig bei Nachweisen, die belegen, dass die festgelegten Verfahren und Massnahmen auch eingehalten werden (hier spricht man von Nachweisdokumenten und der Nachweisdokumentation). So muss beispielsweise die Durchführung von Schulungen oder von internen Audits dokumentiert werden und die für das Unternehmen im Bereich des Datenschutzes und der Datensicherheit relevanten und einzuhaltenden gesetzlichen Grundlagen müssen erfasst werden.

Damit die Dokumentation den Normanforderungen entspricht, muss sie zudem auf Vorgaben beruhen, welche deren Erstellung, Freigabe und Änderung regeln (Dokumentenlenkung). Die Dokumente des DSMS müssen von

den dafür zuständigen Personen oder Organisationseinheiten erstellt, geprüft und freigegeben werden. Auch Änderungen an den Dokumenten dürfen nur im Rahmen eines kontrollierten Prozesses erfolgen, der gewährleistet, dass jeweils die neueste Version eines Dokuments verfügbar ist. Änderungen an Dokumenten sollten nachvollziehbar sein und nicht mehr aktuelle Versionen von Dokumenten sollten noch für eine bestimmte Zeit aufbewahrt werden. Diese Vorgaben werden in der Regel durch den Erlass einer entsprechenden Weisung oder einer anderen verbindlichen Regelung festgehalten.

Die Dokumente des DSMS müssen den betreffenden Mitarbeitenden zugänglich sein, was häufig mittels Publikation des DSMS im Intranet umgesetzt wird. Zudem sind auf dem Markt spezielle Software-Programme erhältlich, welche den zertifizierten Unternehmen die Verwaltung der Dokumente des DSMS erleichtern, da sie Funktionen für die kontrollierte Erstellung, Änderung und Freigabe sowie die Archivierung enthalten. Aufwändiger und weniger geeignet ist die Publikation der Dokumentation des DSMS auf einem Laufwerk, wenn nicht sichergestellt werden kann, dass die Dokumente nicht durch unbefugte Personen geändert oder gelöscht werden können. Nachweisdokumente, welche sensible Informationen enthalten wie beispielsweise eine Liste von Datenschutzvorfällen einschliesslich der eingeleiteten Massnahmen müssen und dürfen natürlich nur den berechtigten Personen zugänglich sein. Daher müssen allenfalls zwei verschiedene Ablagen geführt werden, sofern der Zugriff auf diese Dokumente nicht mittels technischen Massnahmen auf berechtigte Personen eingeschränkt werden kann.

3. Rechtliche Anforderungen

Bei der Umsetzung des DSMS müssen die Datenschutzgrundsätze beachtet werden. Diese sind in den Zertifizierungsrichtlinien in 9 Ziele und insgesamt 20 Massnahmen gegliedert, die wiederum im Leitfaden genauer ausgeführt sind. Allerdings reicht es für die Umsetzung nicht aus, eine entsprechende Datenschutzweisung und/oder weitere Richtlinien oder Policies zu erlassen.

Die Konformität des DSMS mit den Datenschutzgrundsätzen muss im Rahmen eines sogenannten Konformitätsmanagements systematisch sichergestellt werden. Die Erläuterungen zu den Zertifizierungsrichtlinien 2008 enthalten Ausführungen zum Konformitätsmanagement, die für die praktische Umsetzung noch weiterer Erklärungen bedürfen.

Im Rahmen des Konformitätsmanagements geht es darum, durch ein systematisches und geplantes Vorgehen zu gewährleisten, dass bei den Datenbe-

arbeitungen im Geltungsbereich des Zertifikats die Datenschutzgrundsätze eingehalten werden. Werden Abweichungen (der EDÖB spricht von Nicht-Konformitäten) festgestellt, dann müssen Massnahmen zu deren Behebung eingeleitet und auch kontrolliert umgesetzt werden.

Das Konformitätsmanagement sollte sich nicht nur auf die Behebung bereits erfolgter Verstösse beschränken, sondern auch auf deren Verhinderung ausgerichtet sein. Dies kann in der Regel mit den folgenden Massnahmen erreicht werden:

- Zunächst sollten die zu zertifizierenden Datenbearbeitungsverfahren daraufhin überprüft werden, ob die Datenschutzgrundsätze der Zertifizierungsrichtlinien eingehalten werden. Es empfiehlt sich, eine solche Beurteilung für alle zu zertifizierenden Datenbearbeitungsverfahren einzeln vorzunehmen. In der Praxis ist es möglich, dass einzelne Datenschutzgrundsätze nicht anwendbar sind, beispielsweise weil im Zertifizierungsbereich keine Datenweiterleitung ins Ausland stattfindet oder weil keine Datenbearbeitungen geoutsourct werden. In einem solchen Fall sollte der betreffende Datenschutzgrundsatz als nicht anwendbar bezeichnet und diese Beurteilung auch begründet werden.
- Eine Konformitätsprüfung muss auch bei einer allfälligen Änderung oder Neueinführung von Datenbearbeitungsverfahren erfolgen. In diesem Zusammenhang ist zu empfehlen, ein Projektvorgehen zu definieren, bei dem die Frage der Datenschutzrelevanz des Projekts möglichst frühzeitig geprüft wird.
- Das Ergebnis der Konformitätsprüfung muss jeweils dokumentiert und für eine erleichterte Prüfung im Rahmen des Audits durch die Zertifizierungsstelle begründet werden.
- Werden Nicht-Konformitäten festgestellt, müssen geeignete Massnahmen zu deren Behebung bzw. bei neuen Datenbearbeitungsverfahren zu deren Verhinderung eingeleitet und umgesetzt werden. Auch dies ist zu dokumentieren.
- Die Konformitätsprüfung muss regelmässig wiederholt werden. Zu empfehlen ist eine jährliche Wiederholung unter Berücksichtigung der allenfalls geänderten Rahmenbedingungen.
- Kommt es trotz der vorsorglichen Massnahmen und Konformitätsprüfungen zu einer Datenschutzverletzung, muss gewährleistet sein, dass diese systematisch erfasst und behandelt werden. Dazu sollte ein Prozess definiert werden, bei dem klar festgelegt wird, wem vermutete Datenschutzverletzungen gemeldet werden müssen und welche Personen an

der weiteren Bearbeitung mitwirken müssen. Auch hier ist es wichtig, die gemeldeten Vorfälle und die eingeleiteten Massnahmen zu dokumentieren.
- Eine zusätzliche Konformitätsprüfung erfolgt zudem im Rahmen der internen Audits, die regelmässig geplant und durchgeführt werden müssen. Werden dabei Abweichungen von den gesetzlichen Vorgaben oder den Normvorgaben festgestellt, dann müssen diese ebenfalls dokumentiert und behandelt werden.

Um den Überblick über festgestellte oder vermutete Datenschutzverletzungen zu behalten, ist zu empfehlen, diese in einer zentralen, nach Kalenderjahren gegliederten Übersicht zu dokumentieren, die regelmässig aktualisiert wird.

4. Datensicherheit

Bei einer Datenschutzzertifizierung nach VDSZ nimmt der Nachweis, dass die Datensicherheit gewährleistet wird, eine bedeutende Rolle ein. Der Leitfaden enthält die umzusetzenden Massnahmen und verweist dabei auf ausgewählte Massnahmen, die in Anhang A der ISO/IEC 27001:2013 definiert sind.

Der Zusammenhang zwischen Datenschutz und Informationssicherheit mit den in den Zertifizierungsrichtlinien enthaltenen Zielen und Massnahmen sowie den anwendbaren Massnahmen des Anhang A der ISO 27001:2013 zeigt die folgende Grafik, die auf der Website des EDÖB publiziert ist.

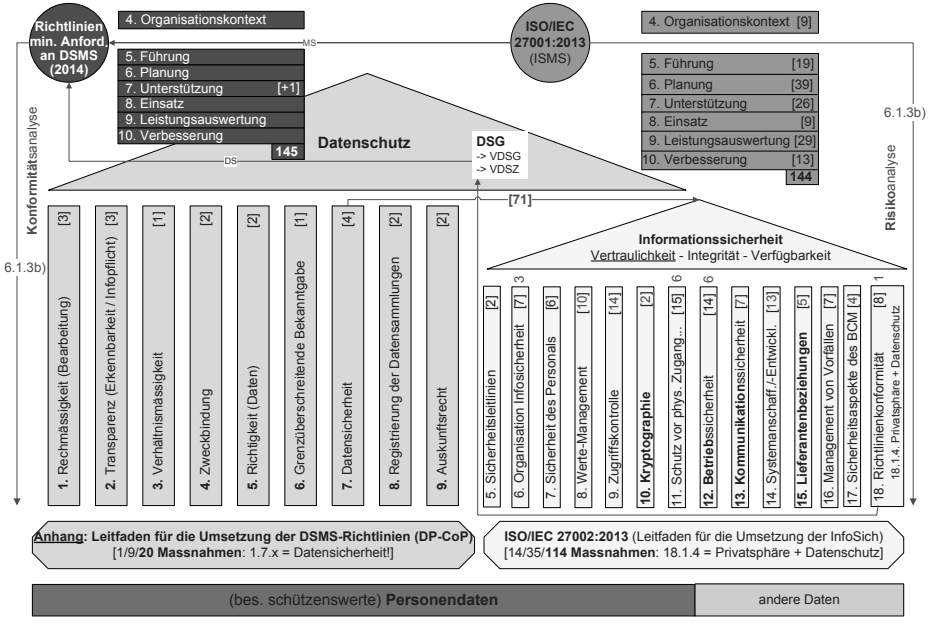

Abbildung 1: Datenschutz versus Informationssicherheit

Ob und wenn ja welche der in den Zertifizierungsrichtlinien genannten Massnahmen einschliesslich der Massnahmen des Anhang A der ISO/IEC 27001:2013 umgesetzt werden müssen, ist durch das Unternehmen auf der Basis einer Risikoanalyse zu bestimmen. Die Gesamtheit aller Massnahmen muss die Datensicherheit gemäss den Vorgaben des DSG gewährleisten, somit im Hinblick auf die festgestellten Risiken angemessen sein[34]. Im Gegensatz zu den Grundsätzen im Bereich des Datenschutzes, bei denen ein Ausschluss von Massnahmen nur dann zulässig ist, wenn diese auf die betreffende Datenbearbeitung nicht anwendbar ist, hat das Unternehmen im Bereich der zu ergreifenden Datensicherheitsmassnahmen daher einen grösseren Handlungsspielraum.

Auch im Bereich der Datensicherheitsmassnahmen spielt die Dokumentation der anwendbaren und umgesetzten Massnahmen eine sehr wichtige Rolle. In der sogenannten „Anwendbarkeitserklärung“ (auch „Statement of Applicabi-

34 Art. 7 DSG i.V.m. Art. 8-10 VDSG.

lity“ oder kurz SoA genannt), muss zu jeder gemäss dem Leitfaden des EDÖB grundsätzlich anwendbaren Massnahmen des Anhangs A der ISO/IEC 27001:2013 eine Aussage zu deren Anwendbarkeit für den zertifizierten Bereich gemacht werden. Wird eine Massnahme als nicht anwendbar bezeichnet, dann muss dies begründet werden. Die Zertifizierungsstelle prüft anhand der Anwendbarkeitserklärung, ob und wie die als anwendbar bezeichneten Kontrollen umgesetzt wurden. Zudem werden auch die als nicht anwendbar bezeichneten Kontrollen hinterfragt. Probleme bereitet den Unternehmen teilweise die Beurteilung der Anwendbarkeit von Massnahmen, die durch einen Outsourcingpartner erfüllt werden müssen, da sie einen ausgelagerten Datenbearbeitungsprozess betreffen. Diese werden in der Anwendbarkeitserklärung häufig entgegen den anwendbaren rechtlichen Grundlagen als „nicht anwendbar“ bezeichnet. Lagert das Unternehmen einen Datenbearbeitungsprozess im Geltungsbereich des zu zertifizierenden DSMS an einen Outsourcingpartner aus, dann bleibt es gegenüber den betroffenen Personen dafür verantwortlich, dass der Outsourcingpartner Datenschutz und Datensicherheit gewährleistet[35]. Daher sind auch solche Massnahmen als anwendbar zu bezeichnen und deren Umsetzung muss beim Outsourcingpartner kontrolliert werden.

Insgesamt muss in der Anwendbarkeitserklärung eine sehr grosse Zahl von Massnahmen geprüft und beurteilt werden. Zur Erstellung der Anwendbarkeitserklärung kommt in der Regel aber noch der oft weit grössere Aufwand für die Umsetzung und die Dokumentation derjenigen Massnahmen, die zwar anwendbar, aber noch nicht umgesetzt sind oder deren Umsetzung noch nicht dokumentiert wurde. Zudem muss eine Risikoanalyse durchgeführt und ein entsprechender Prozesses implementiert werden, falls ein solcher noch nicht vorhanden ist.

[35] Art. 10a DSG.

V. Die Zertifizierung des Datenschutz-Managementsystems

1. Vorbereitung und Planung

Die Durchführung des Zertifizierungsaudits wird gemeinsam mit der Zertifizierungsstelle geplant. In der Regel finden ein oder mehrere Vorgespräche sowie ein Voraudit statt, in dem abgeklärt wird, ob die Normanforderungen erfüllt sind und das DSMS bereits Zertifizierungsreife erlangt hat. Ist dies der Fall, dann wird auf der Basis des dokumentierten Geltungsbereichs des DSMS das Auditprogramm erstellt. Dabei werden alle zu zertifizierenden Datenbearbeitungsprozesse, Organisationseinheiten, Standorte, technischen Infrastrukturen und Outsourcingpartner mitberücksichtigt. Anhand des Auditprogramms wissen die betroffenen Mitarbeitenden im Unternehmen, wann und zu welchen Themen sie befragt werden.

2. Durchführung

Die Durchführung des Audits umfasst allgemein gesagt die Prüfung, ob die Dokumentation, die Datenbearbeitungsprozesse und die Massnahmen der Datensicherheit den gesetzlichen und den Normanforderungen entsprechen. Die relevante Dokumentation des DSMS muss den Auditorinnen und Auditoren rechtzeitig (d.h. in der Regel rund 2 Wochen) vor dem Audit zur Verfügung gestellt werden und wird von diesen vorgängig im Rahmen des Dokumentenaudits geprüft. Auf der Basis des Auditprogramms finden am Zertifizierungsaudit, das je nach Umfang einen oder mehrere Tage dauert, Befragungen der zuständigen Mitarbeitenden statt. Zudem werden Datenbearbeitungsverfahren sowie die Umsetzung von Datensicherheitsmassnahmen unter Berücksichtigung der Dokumentation des DSMS vor Ort geprüft.

3. Resultat des Audits

Das Resultat des Zertifizierungsaudits wird im Bericht der Zertifizierungsstelle zusammengefasst. Stellt die Zertifizierungsstelle keine Abweichungen von den Normvorgaben fest, dann wird das Zertifikat erteilt, das 3 Jahre gültig ist[36]. Nach Ablauf der Gültigkeitsfrist muss das Zertifizierungsverfahren

[36] Art. 6 Abs. 2 VDSZ.

erneuert werden. In der Zwischenzeit prüft die Zertifizierungsstelle jährlich mittels Stichproben, ob das DSMS die Normvorgaben noch erfüllt[37].

Werden anlässlich eines Zertifizierungsaudits wesentliche, zertifikatsverhindernde Abweichungen von den Normvorgaben festgestellt (sogenannte Major-Non-Conformities), dann wird das Zertifikat nicht erteilt. Werden weniger schwerwiegende Mängel festgestellt (Minor-Non-Conformities), dann wird das Zertifikat zwar erteilt, der Mangel muss aber bis zum nächsten Audit behoben werden, widrigenfalls dieser zu einem wesentlichen Mangel wird.

Die folgende Abbildung gibt einen Überblick über den Zertifizierungszyklus[38].

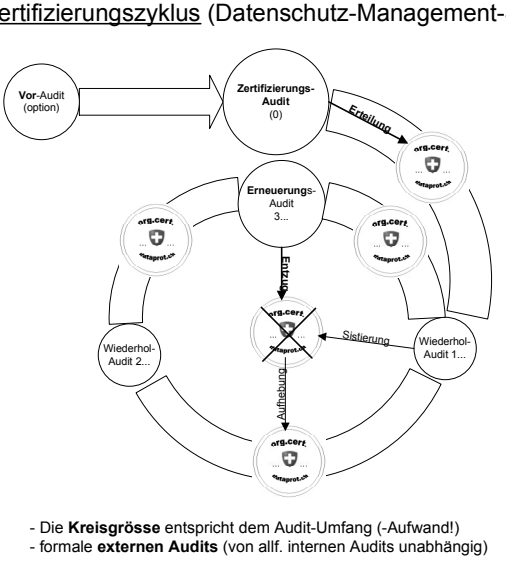

Abbildung 2: Zertifizierungszyklus

37 Art. 6 Abs. 2 VDSZ

38 Quelle: EDÖB, abrufbar unter http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html, besucht am 03.01.2016.

4. Sistierung und Entzug des Zertifikats

Wesentliche Mängel, die im Rahmen der jährlichen summarischen Prüfung oder bei einem Rezertifizierungsaudit festgestellt werden, führen zu einem Entzug oder einer Sistierung des Zertifikats[39]. Wurde dem EDÖB die Zertifizierung gemeldet, dann muss ihm dies sowohl vom zertifizierten Unternehmen als auch von der Zertifizierungsstelle gemeldet werden.

Stellt der EDÖB im Rahmen seiner Aufsichtstätigkeit[40] bei einem zertifizierten Unternehmen schwere Mängel fest, dann informiert er die Zertifizierungsstelle darüber. Diese ist verpflichtet, das zertifizierte Unternehmen aufzufordern, die Mängel innerhalb von 30 Tagen zu beheben, widrigenfalls die Zertifizierungsstelle das Zertifikat sistieren muss. Besteht keine Aussicht auf die Behebung des schweren Mangels innerhalb einer angemessenen Frist, dann muss die Zertifizierungsstelle das Zertifikat entziehen. Wird der schwere Mangel nicht behoben und das Zertifikat von der Zertifizierungsstelle weder sistiert noch entzogen, dann erlässt der EDÖB eine Empfehlung an das zertifizierte Unternehmen und/oder an die Zertifizierungsstelle. Im letzteren Fall informiert er zudem die SAS[41].

Das in der VDSZ festgelegte Vorgehen bei durch den EDÖB festgestellten schweren Mängeln führt in der Praxis insbesondere aus folgenden Gründen zu Problemen:

- Die 30tägige Frist ist in den meisten Fällen zu kurz, um einen schweren Mangel beheben zu können. Dies ist insbesondere dann der Fall, wenn für die Herstellung eines gesetzes-, bzw. normkonformen Zustands organisatorische Abläufe angepasst werden müssen oder Anpassungen an der IT-Infrastruktur (Hardware oder Software) erforderlich sind.
- Ein schwerer Mangel liegt vor, wenn wesentliche Voraussetzungen der Datenschutzzertifizierung nicht mehr erfüllt sind oder eine Zertifizierung in irreführender oder missbräuchlicher Art und Weise verwendet wird[42]. Schwere Mängel können beispielsweise vorliegen, wenn keine internen Audits durchgeführt werden oder das DSMS

[39] Art. 9 Abs. 1 VDSZ.
[40] Art. 27 oder 29 DSG.
[41] Art. 10 VDSZ.
[42] Art. 9 Abs. 1 VDSZ.

unvollständig ist oder nicht gepflegt und weiterentwickelt wird. Ein schwerer Mangel kann aber auch in unzureichenden Massnahmen zur Gewährleistung der Datensicherheit bestehen oder in einer nicht gesetzeskonformen Datenbearbeitung. Die Frage, ob tatsächlich ein schwerer Mangel vorliegt, kann strittig sein.

- Stellt der EDÖB einen seiner Beurteilung nach schweren Mangel fest und teilt das zertifizierte Unternehmen diese Einschätzung nicht, dann ist das in Art. 10 VDSZ festgelegte Vorgehen problematisch und führt zu Rechtsunsicherheiten. Dies ist insbesondere dann der Fall, wenn der durch den EDÖB festgestellte schwere Mangel auf einer datenschutzrechtlichen Beurteilung eines Sachverhalts basiert, den das zertifizierte Unternehmen anders beurteilt. Die Beurteilung des EDÖB hat für das zertifizierte Unternehmen keine unmittelbar bindende Wirkung. Erlässt der EDÖB eine Empfehlung an das betreffende Unternehmen und hält dieses sich nicht daran oder lehnt es die Empfehlung ab, steht dem EDÖB der Weg vor Bundesverwaltungsgericht offen[43]. Das in der VDSZ festgelegte Verfahren führt aber dazu, dass das Datenschutzzertifikat durch die Zertifizierungsstelle entzogen werden muss, bevor die Frage, ob überhaupt ein schwerer Mangel vorliegt, gerichtlich beurteilt wurde. Dies ist insbesondere in Fällen, in denen die Datenschutzzertifizierung gesetzlich verpflichtend vorgeschrieben ist, unbefriedigend und führt zu Rechtsunsicherheiten. Wird beispielsweise einem Krankenversicherer das Zertifikat für die Datenannahmestelle entzogen, dann dürften Spitäler keine DRG-Rechnungen mehr an den Krankenversicherer senden. Dies führt letztendlich dazu, dass die Spitäler ihre Kosten nicht ersetzt bekommen.
- Entzieht die Zertifizierungsstelle das Zertifikat entgegen der Bestimmung von Art. 10 Abs. 3 VDSZ nicht, dann richtet der EDÖB eine entsprechende Empfehlung an die Zertifizierungsstelle und informiert die SAS[44]. Zurzeit ist es unklar, welche Konsequenzen dies im Hinblick auf die Akkreditierung der Zertifizierungsstelle haben kann.

---

43 Art. 29 Abs. 4 DSG.

44 Art. 10 Abs. 4 VDSZ.

Es ist zu hoffen, dass die VDSZ in diesem Bereich bald angepasst wird, zumal zu erwarten ist, dass in Zukunft noch weitere gesetzlich verpflichtende Datenschutzzertifizierungen eingeführt werden.

Generell ist zu empfehlen, dass ein zertifiziertes Unternehmen in einem solchen Fall aktiv sowohl mit dem EDÖB als auch mit der Zertifizierungsstelle kommuniziert. Auch wenn eine Behebung von Mängeln innerhalb von 30 Tagen nicht möglich sein sollte, so muss innerhalb dieser Frist in jedem Fall mitgeteilt werden, ob der Mangel durch das zertifizierte Unternehmen anerkannt wird und mit welchen Massnahmen dieser bis wann behoben wird.

VI. Anhang

Checkliste: Wichtige Checkpunkte für die Planung, den Aufbau, die Einführung und die Zertifizierung eines DSMS in der Praxis

Die folgende Checkliste enthält eine nicht abschliessende Auflistung von wichtigen Tätigkeiten im Hinblick auf die Zertifizierung eines DSMS nach VDSZ. Nicht enthalten sind alle Tätigkeiten, die den Betrieb des DSMS nach der erfolgreichen Zertifizierung betreffen.

Phase	**Tätigkeiten**
Planung	Studium der Norm – VDSZ – Zertifizierungsrichtlinien – Leitfaden zum DSMS – Erläuterungen zu den Zertifizierungsrichtlinien 2008 – Erläuterungen zu den Zertifizierungsrichtlinien 2014 – ISO/IEC 27001:2013
	Aufwandschätzung – Soll/Ist-Vergleich zwischen den Normanforderungen und den vorhandenen Dokumenten und Prozessen – Einschätzung der erforderlichen internen und externe personellen Ressourcen
	Auswahl der Zertifizierungsstelle

	– Rechtzeitige Kontaktaufnahme mit akkreditierter Zertifizierungsstelle – Klärung der Kosten der Zertifizierung – Vertragsabschluss – Zeitliche Planung des Zertifizierungsaudits
	Festlegung des Geltungsbereichs des DSMS – Zu zertifizierende Datenbearbeitungsverfahren (Art. 4 Abs. 1 VDSZ: alle oder einzelne, abgegrenzte Datenbearbeitungsverfahren) – Bezeichnung der relevanten Datensammlungen – Bezeichnung der Standorte, an denen die zu zertifizierenden Datenbearbeitungsverfahren erbracht werden – Bezeichnung der geoutsourcten Datenbearbeitungsverfahren und der Outsourcingpartner – Bezeichnung der im zu zertifizierenden Bereich verwendeten IT-Infrastruktur und Technologien
Aufbau und Einführung	Dokumentation – Erlass von Vorgaben für die Erstellung, und die Änderung von Dokumenten inklusive Freigabe und Archivierung (Weisung Dokumentenlenkung) – Erstellung der Vorgabe- und Nachweisdokumente gemäss Normanforderungen – Freigabe der Vorgabe- und Nachweisdokumente gemäss internen Vorgaben (Weisung Dokumentenlenkung) – Publikation der Vorgabe- und Nachweisdokumente auf dem Intranet oder in anderer geeigneter Weise
	Rechtliche Anforderungen – Erlass einer Datenschutzpolitik – Erlass von Weisungen und Policies betr. Datenschutz – Erstellung eines Prozesses betr. Konformitätsmanagement – Kontrolle der Konformität der zu zertifizierenden Datenbearbeitungsverfahren mit den Datenschutzgrundsätzen gemäss Zertifizierungsrichtlinien – Kontrolle von geplanten oder geänderten Datenbearbeitungsverfahren: Frühzeitige Klärung der Datenschutzrelevanz von Projekten – Planung und Durchführung von internen Audits – Festlegung von Massnahmen zur Beseitigung von festgestellten Nicht-Konformitäten und Kontrolle von deren Umsetzung

	– Führen einer zentralen Übersicht über die festgestellten Nicht-Konformitäten und den Stand der Umsetzung der definierten Massnahmen
	Datensicherheit – Erlass von Weisungen und Policies im Bereich Datensicherheit – Planung und Durchführung eines Risikomanagements – Erstellung der Anwendbarkeitserklärung (Statement of Applicability, SoA) – Umsetzung der in der SoA als anwendbar erklärten Massnahmen
Zertifizierung	Vorbereitung des Zertifizierungsaudits mit der Zertifizierungsstelle – Planung des Auditprogramms auf der Basis des definierten Geltungsbereichs des DSMS – Information der am Audit beteiligten Personen inklusive Outsourcingpartnern – Rechtzeitige Zustellung der Dokumente des DSMS an Zertifizierungsstelle
	Zertifizierungsaudit – Beantwortung von Fragen – Vorführen von Datenbearbeitungsverfahren – Gewährleistung des Zugangs zu Räumen und Systemen – Ermöglichung der Kontrolle von Datensicherheitsmassnahmen
	Nachbereitung – Meldung der erfolgreichen Zertifizierung an den EDÖB, falls eine Befreiung von der Meldepflicht für Datensammlungen erfolgen soll (Art. 11a Abs. 5 lit. f DSG) – Behebung von allfälligen Nicht-Konformitäten gemäss Auditbericht

Tabelle 1: Checkliste: Wichtige Checkpunkte für die Planung, den Aufbau, die Einführung und die Zertifizierung eines DSMS nach VDSZ in der Praxis