Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

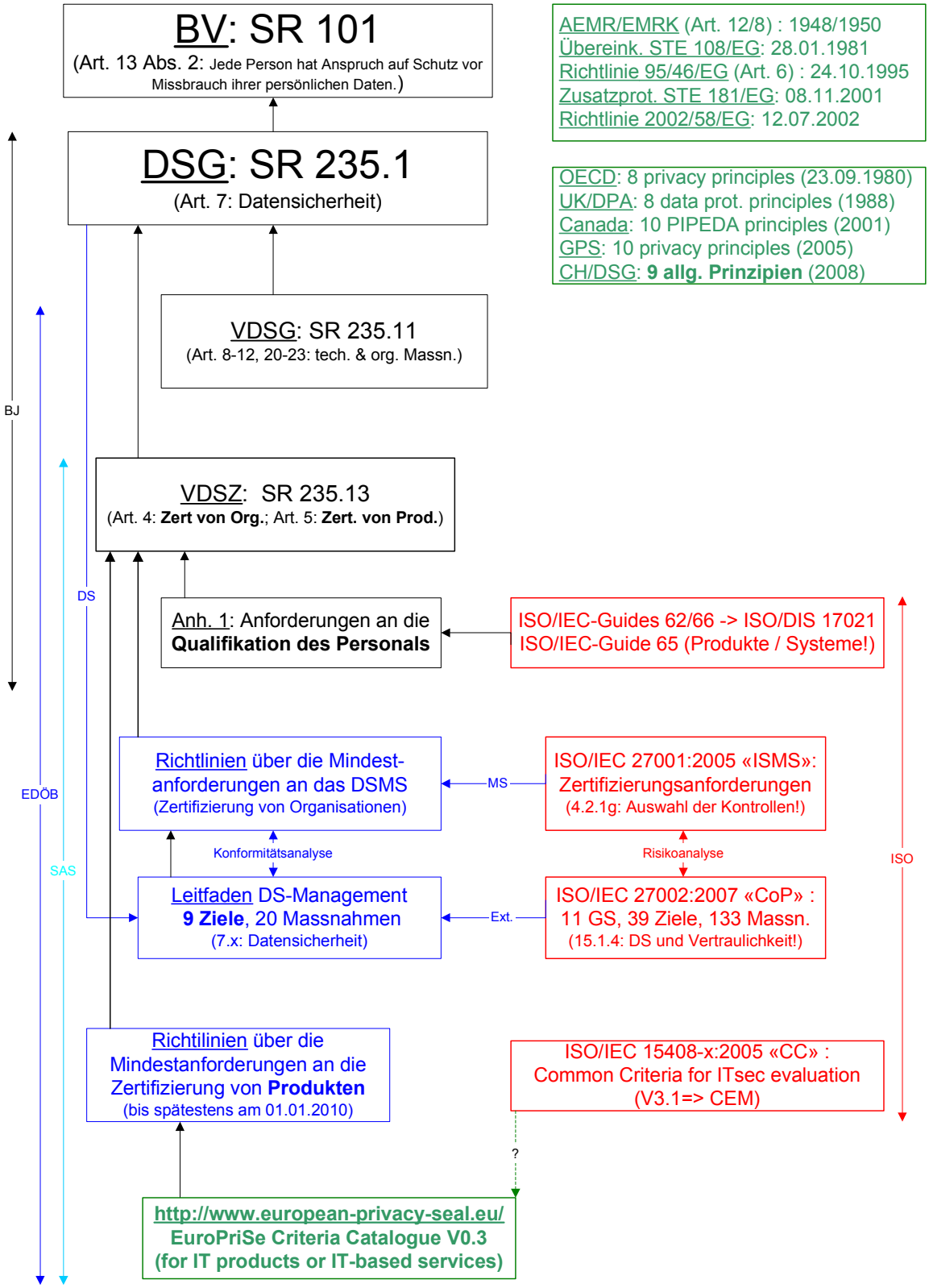
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Erläuterungen zu den «Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem (DSMS)»

Die «Richtlinien betreffend die Mindestanforderungen an das Datenschutzmanagementsystem» führen Art. 4 Abs. 3 der Verordnung über die Datenschutzzertifizierungen (VDSZ; SR 235.13) aus. Die erwähnte Delegationsnorm von Art. 4 Abs. 3 VDSZ hält fest, dass beim Erlass der Richtlinien internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen insbesondere die Normen ISO 9001:2000 und 27001:2005 zu berücksichtigen sind. Mit diesen Vorgaben, und um ein von den Spezialisten bereits bekanntes und benutztes Instrument zur Verfügung zu stellen, hat sich der EDÖB bei der Erstellung seiner Richtlinien an die Anforderungen an Managementsysteme im Allgemeinen angelehnt. Gleichzeitig wurde sichergestellt, dass das Schwergewicht auf die Datenschutz-Aspekte gelegt wurde.

Nachfolgende Darstellung dient dazu, die DSMS-Richtlinien im Kontext der schweizerischen Rechtsordnung mit Hinweisen auf die europäische Datenschutzgesetzgebung dazustellen, sowie die Parallelen zu den entsprechenden ISO-Normen aufzuzeigen. Der Einfachheit halber wurden darin die «Richtlinien darüber, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind», die der EDÖB bis spätestens am 1. Januar 2010 zu erlassen hat, weggelassen:

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

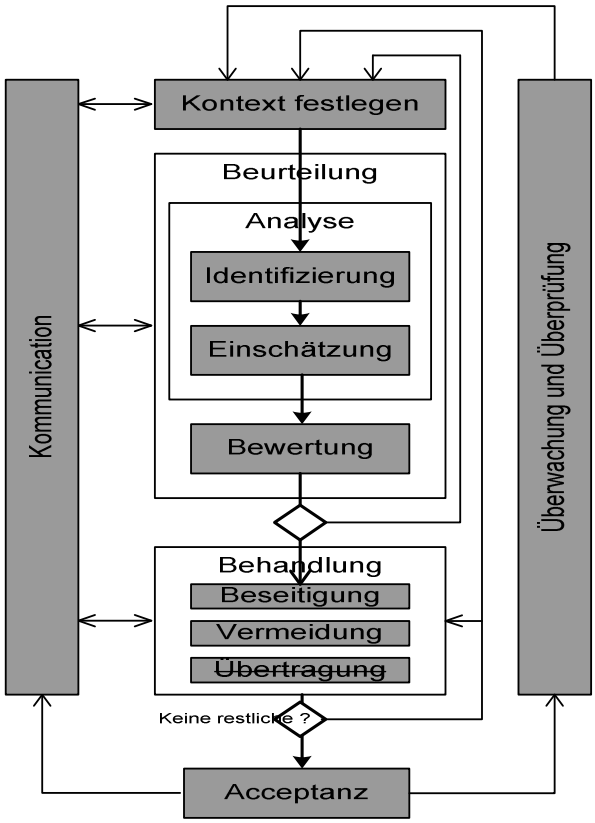

BV: SR 101
(Art. 13 Abs. 2: Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.)
DSG: SR 235.1
(Art. 7: Datensicherheit)
VDSG: SR 235.11
(Art. 8-12, 20-23: tech. & org. Massn.)
VDSZ: SR 235.13
(Art. 4: Zert von Org.; Art. 5: Zert. von Prod.)
Anh. 1: Anforderungen an die Qualifikation des Personals
Richtlinien über die Mindest-anforderungen an das DSMS
(Zertifizierung von Organisationen)
Leitfaden DS-Management
9 Ziele, 20 Massnahmen
(7.x: Datensicherheit)
Richtilinien über die Mindestanforderungen an die Zertifizierung von Produkten
(bis spätestens am 01.01.2010)
http://www.european-privacy-seal.eu/
EuroPriSe Criteria Catalogue V0.3
(for IT products or IT-based services)
AEMR/EMRK (Art. 12/8) : 1948/1950
Übereink. STE 108/EG: 28.01.1981
Richtlinie 95/46/EG (Art. 6) : 24.10.1995
Zusatzprot. STE 181/EG: 08.11.2001
Richtlinie 2002/58/EG: 12.07.2002
OECD: 8 privacy principles (23.09.1980)
UK/DPA: 8 data prot. principles (1988)
Canada: 10 PIPEDA principles (2001)
GPS: 10 privacy principles (2005)
CH/DSG: 9 allg. Prinzipien (2008)
ISO/IEC-Guides 62/66 -> ISO/DIS 17021
ISO/IEC-Guide 65 (Produkte / Systeme!)
ISO/IEC 27001:2005 «ISMS»: Zertifizierungsanforderungen
(4.2.1g: Auswahl der Kontrollen!)
ISO/IEC 27002:2007 «CoP» : 11 GS, 39 Ziele, 133 Massn.
(15.1.4: DS und Vertraulichkeit!)
ISO/IEC 15408-x:2005 «CC» : Common Criteria for ITsec evaluation
(V3.1=> CEM)
MS
Ext.
Konformitätsanalyse
Risikoanalyse
?
BJ
DS
EDÖB
SAS
ISO

In einem ersten Schritt wurden somit die allgemeinen Anforderungen an Managementsysteme aus ISO 27001 übernommen. Diese stammen ihrerseits von den Hauptanforderungen von ISO 9001, wie dies aus dem informativen Anhang C von ISO 27001 hervorgeht. Um in den Richtlinien den Schwerpunkt Datenschutz zu erreichen, wurde allgemein die Risikoanalyse gemäss ISO durch die Einführung einer (**Nicht-)Konformitätsanalyse** ergänzt und spezifisch **bestimmte ISO-27001-Klauseln**, die den Aufbau und die Dokumentation des DSMS betreffen, speziell **auslegt**.

Die Hauptschwierigkeit bestand – wie erwähnt – darin, den Akzent mehr auf den Datenschutz als allein auf die Informationssicherheit zu setzen. Im Bundesgesetz über den Datenschutz (DSG; SR 235.1) regelt Art. 7 die Datensicherheit. Gestützt auf diesen Artikel kann man den Datenschutz als globales Ziel betrachten, das durch Ausdehnung das Ziel der in ISO 27001 verfolgten Datensicherheit abdeckt. Die Richtlinien sollen dazu dienen, ein Datenschutzmanagementsystem zu erstellen, das unter anderem folgende Elemente enthält: eine *Politik des DSMS*, eine *Auswahl von Massnahmen für die Behandlung von Nichtkonformitäten*, eine *Anwendbarkeitserklärung* der umgesetzten Massnahmen mit einer Begründung derjenigen, die ausgeschlossen wurden, ein *Behandlungsplan der Nichtkonformitäten*, eine *Überprüfung/Nachprüfung der Datenschutz-Verletzungen oder –Zwischenfälle*, und die *Korrektur- oder Vorbeugungsmassnahmen zur Verbesserung des DSMS*.

Eine weitere Schwierigkeit bestand in der Tatsache, dass beim ISMS das Risikomanagement den Ausgangspunkt bildet. Ein solches Risikomanagement mag sich gut für die beim ISMS vorgesehenen freiwilligen Informationssicherheitsziele eignen, allerdings trifft dies gar nicht auf die gesetzlichen Datenschutzvoraussetzungen zu. Denn entweder ist etwas datenschutzkonform oder nicht. Aus diesem Grund drängte es sich auf, neben dem Risikomanagement ein Konformitätsmanagement aufzunehmen, wobei ersteres im Zusammenhang mit der Datensicherheit bestehen bleibt (vgl. Prinzip/Ziel/Artikel 7).

Konkret gestaltet sich die Methode für eine **Beurteilung der Nichtkonformität** wie folgt: Zunächst erfolgt eine **Analyse** der Nichtkonformität (*Identifizierung* der Ursachen und *Einschätzung* der Nichtkonformität), die in eine **Bewertung** der Nichtkonformität mündet. Letztere basiert in der Regel auf einer Skala mit folgenden zwei Werten: leichte oder erhebliche Nichtkonformität. Wir kommen dann zur **Behandlung** der Nichtkonformitäten**,** zwar zu ihrer **Beseitigung** durch angemessene Massnahmen oder zu ihrer **Vermeidung** beispielsweise durch Verzicht auf die entsprechende Bearbeitung. Im Gegensatz zur Risikoanalyse kann eine Nichtkonformität weder übertragen noch akzeptiert (keinerlei restliche Nicht-Konformität) werden.

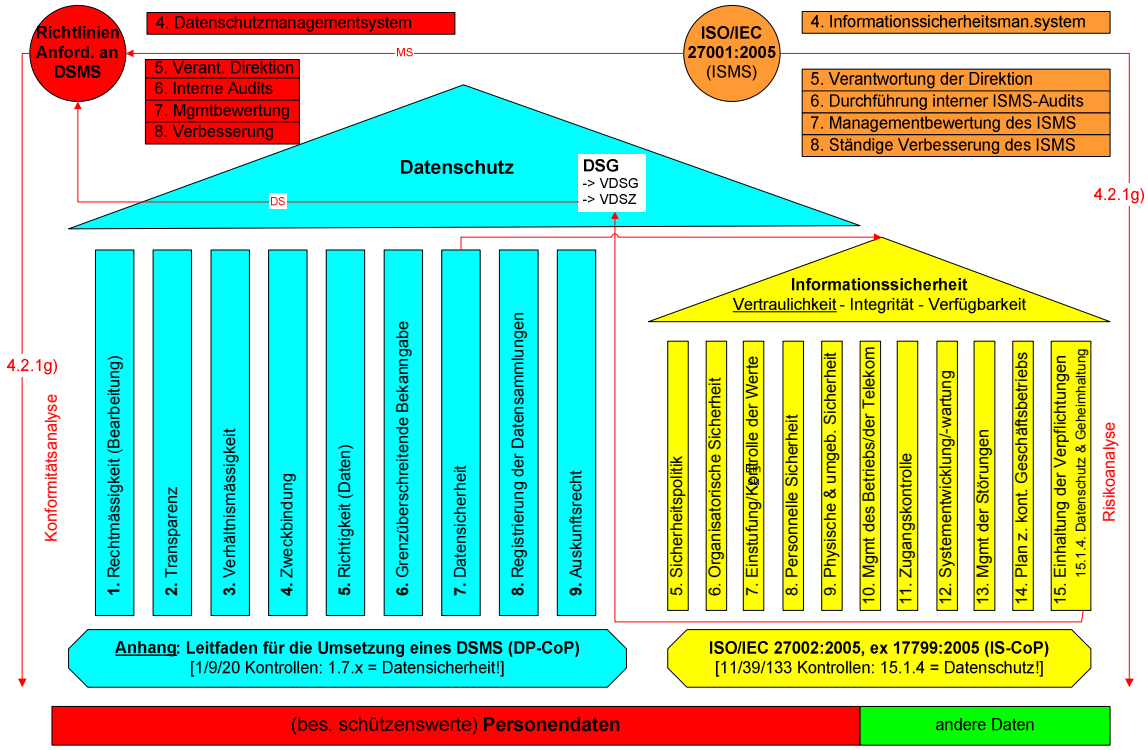


In einem zweiten Schritt ging es darum, den normativen Anhang A von ISO 27001 zu übernehmen, der im Grunde genommen aus dem Inhaltsverzeichnis der Norm ISO/IEC 27002:2005 besteht (bekannter unter dem Namen «Leitfaden zum Management von Informationssicherheit»). Letztere setzt sich aus 15 Kapiteln zusammen, wovon die 11 letzten die «Kontrollgruppen» bilden, die ihrerseits in 39 «Kontrollziele» unterteilt sind und zu insgesamt 133 «Kontrollmassnahmen» führen. Der **Schwerpunkt Datenschutz** in ISO ergibt sich einzig aus der **Massnahme 15.1.4**, die den «Datenschutz und Vertraulichkeit von personenbezogenen Informationen» betrifft, und die in der Substanz vorschreibt, dass „diese gemäss den Rechtsnormen, Reglementen und allfällig anwendbaren Vertragsbestimmungen gewahrt sein müssen.» Um daraus eine Datenschutzzertifizierung von Organisationen oder Verfahren erreichen zu können, muss diese sehr allgemeine Massnahme 15.1.4 offensichtlich verstärkt, detailliert und in Ziele unterteilt werden, die ihrerseits durch konkrete Datenschutzmassnahmen erreicht werden können. Dies wurde mit dem «**Leitfaden für das Datenschutz-Management**» verwirklicht, dessen Ziele und Massnahmen in Ziffer 5 der «**Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem**» zusammengefasst und im Anhang zu den DSMS-Richtlinien ausführlicher aufgeführt wurden. Mit anderen Worten entspricht das Verhältnis «Leitfaden für das Datenschutz-Management» zu den DSMS-Richtlinien dem Verhältnis ISO 27002 zu ISO 27001.

Analog der OECD und gewissen Ländern wie Australien, Kanada und Grossbritannien, haben wir **«9 allgemeine Grundsätze aus dem Datenschutzgesetz»** als Hauptzweck dieses «Leitfadens für das Datenschutz-Management» definiert. Diese Grundsätze bestehen aus 20 konkreten Datenschutzmassnahmen, die in nicht abschliessender Art die wichtigsten Voraussetzungen enthalten, die dem Gesetz oder seiner Vollzugsverordnung entspringen.

Zum besseren Verständnis dieses Anhangs wurde jede Massnahme gemäss dem Standard ISO 27002 strukturiert (Massnahme, Umsetzung und andere Informationen). Gleich wie die ISMS-Mass-

nahme 15.1.4 auf ein DSMS verweist, muss hier noch hervorgehoben werden, dass das 7. Ziel «Datensicherheit» mit seinen assoziierten Massnahmen nichts anderes als ein Verweis des DSMS auf ein ISMS ist. Somit wurde von den 133 bestehenden Sicherheitsmassnahmen aus ISO 27002 eine Vorselektion der für die Datensicherheit nach DSG relevantesten Massnahmen gemacht.



Auch wenn es natürlich nicht darum geht, für den Erhalt einer DSMS-Zertifizierung eine ISMS-Zertifizierung vorauszusetzen, wird die Zertifizierungsstelle von Fall zu Fall entscheiden müssen, inwieweit eine bereits bestehende ISMS-Zertifizierung, insbesondere was die Anforderungen an die «Datensicherheit» betrifft, anerkannt werden kann. Betreffend die Akkreditierung durch die SAS ist angesichts des engen und ausdrücklichen Bezugs zu den Anforderungen dieser Norm davon auszugehen, dass die DSMS-Akkreditierung als Erweiterung der ISMS-Akkreditierung (ISO 27001) vorgesehen sein wird.

Es ist zu betonen, dass der zurzeit bestehende enge Bezug zu den internationalen Normen ISO 27001 und 27002 für alle betroffenen Akteure (Akkreditierer, Zertifizierungsstellen, zertifizierte Stellen, Auditoren, Kontrolleure) vernünftig und vorteilhaft ist. Die erwähnten Normen kennen eine grosse Anerkennung und Durchdringung des Weltmarktes und leisten vorliegend einen wertvollen terminologischen, strukturellen und systematischen Beitrag. Dieser normative Kontext wird übrigens bald ausgewietet werden durch zusätzliche Leitfäden wie ISO 27003 «Umsetzung des ISMS», ISO 27004 «Metrik und Effizienz der Massnahmen», ISO 27005 «Risikomanagement», ISO 27006 «Akkreditierungsvoraussetzungen» oder noch ISO 27007 «ISMS-Audits» wovon das DSMS profitieren können wird.