# Erläuterungen zu den Änderungen vom 19. März 2014 der «Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem»

**Gestützt auf die Verordnung über Datenschutzzertifizierungen (Art. 4 Abs. 3 VDSZ) erlässt der EDÖB Richtlinien über die Mindestanforderungen an Datenschutzmanagementsysteme (nachfolgend DSMS-Richtlinien). Eine erste Fassung dieser Richtlinien trat am 1. September 2008 in Kraft und lehnte sich stark an die Norm ISO/IEC 27001:2005 an. Diese ist inzwischen durch die am 1. Oktober 2013 veröffentlichte Norm ISO/IEC 27001:2013 ersetzt worden. Bei den Änderungen handelt es sich vor allem um eine fachliche Überarbeitung der verschiedenen Anforderungen an die Informationssicherheit. Gleichzeitig wurde sie an die anderen ISO-Normen betreffend Managementsysteme angepasst. Aufgrund des engen Bezugs der DSMS-Richtlinien zur Norm 27001 drängte sich ihre Anpassung auf. Mit den Änderungen vom 19. März 2014 hat der EDÖB diesen Schritt vollzogen und die Richtlinien an die Norm ISO/IEC 27001:2013 angeglichen.**

## Zu den Änderungen im Einzelnen:

### Bezeichnung der ISO-Norm 27001

Zunächst wurde überall der Begriff «ISO/IEC 27001:2005» durch «ISO/IEC 27001:2013» ersetzt.

### Ziffer 2. Definitionen

Die Kapitel 3.1-3.16 der ISO-Norm 27001 wurden neu zu den Ziffern 2.1.-2.89 der Norm ISO/IEC 27000:2014. Die Verweise wurde in den DSMS-Richtlinien entsprechend geändert.

Bei den Definitionen wurden die Umschreibungen der verschiedenen Begriffe an die neuen Formulierungen der ISO-Norm 27000 angepasst.

### Ziffer 4. Umsetzung (Mindestanforderungen) und Fussnote 6

In Buchstabe b wurden die Bezeichnungen der Ziffern der ISO-Norm entsprechend den neuen Ziffern der Norm ISO/IEC 27001:2013 angepasst. So wurde Ziffer 4.2.1.a. zu 4.3, Ziffer 4.2.1.b zu 5.2, Ziffer 4.2.1.d 1. zu 6.1.2.c.2., Ziffer 4.2.1.g. zu 6.1.3.b. und Ziffer 4.3.1.j. zu 7.5.1.c.

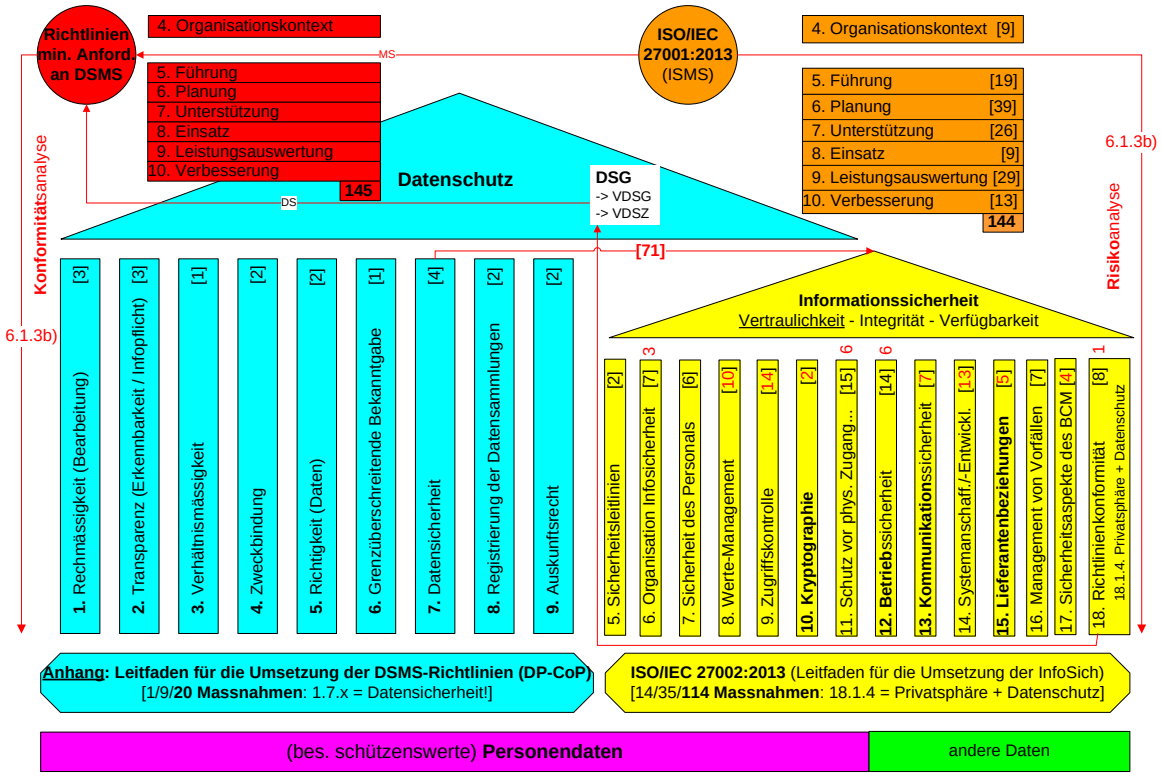
Zudem wurde in Buchstabe b bei Ziffer 5.2 (bisher 4.2.1.b) der Begriff «DSMS-Leitlinie» durch «Datenschutzleitlinie» ersetzt und eine neue Fussnote hinzugefügt. In der Fussnote (Nr. 6) wird präzisiert, dass diese übergeordnete Datenschutzleitlinie durch andere thematische Leitlinien zur Informationssicherheit oder zum Privatsphärenschutz (Beschreibung der Massnahme A.5.1.1) ergänzt wird.

### Ziffern 6. Aufhebung eines anderen Erlasses und 7. Übergangsbestimmung

Die DSMS-Richtlinien vom 19. März 2014 ersetzen diejenigen vom 16. Juli 2008. Aus diesem Grund werden letztere aufgehoben. Wie die Übergangsbestimmung von Ziffer 7 präzisiert, gelten für hängige Zertifizierungsverfahren noch die alten Richtlinien. Diese Verfahren müssen allerdings bis zum 1. Oktober 2014 abgeschlossen sein. Die Zertifizierungsstellen erhalten somit genügend Zeit, um ihre einschlägigen Unterlagen und Verfahren anzupassen. Dieses Datum entspricht auch dem Zeitpunkt, bis zu dem noch nach der alten Norm zertifiziert werden kann. Es ist zu erwarten, dass die Anpassung an ISO/IEC 27001:2013 ohne grosse Schwierigkeiten erfolgen wird. Desgleichen sollte auch die Anpassung der DSMS-Zertifizierungsverfahrens an die neuen DSMS-Richtlinien vom 19. März 2014 keine besonderen Schwierigkeiten bereiten.

Was die Auslegung und Anwendung der neuen Richtlinien betrifft, kann auf die bisherigen Erläuterungen zu den «Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem (DSMS)» aus dem Jahr 2008 verwiesen werden, insbesondere in Bezug auf die (Nicht-)Konformitätsanalyse, die Beurteilung der Nichtkonformität (Bewertung, Behandlung, Beseitigung, Vermeidung) und das Verhältnis der DSMS-Richtlinien zum Anhang.

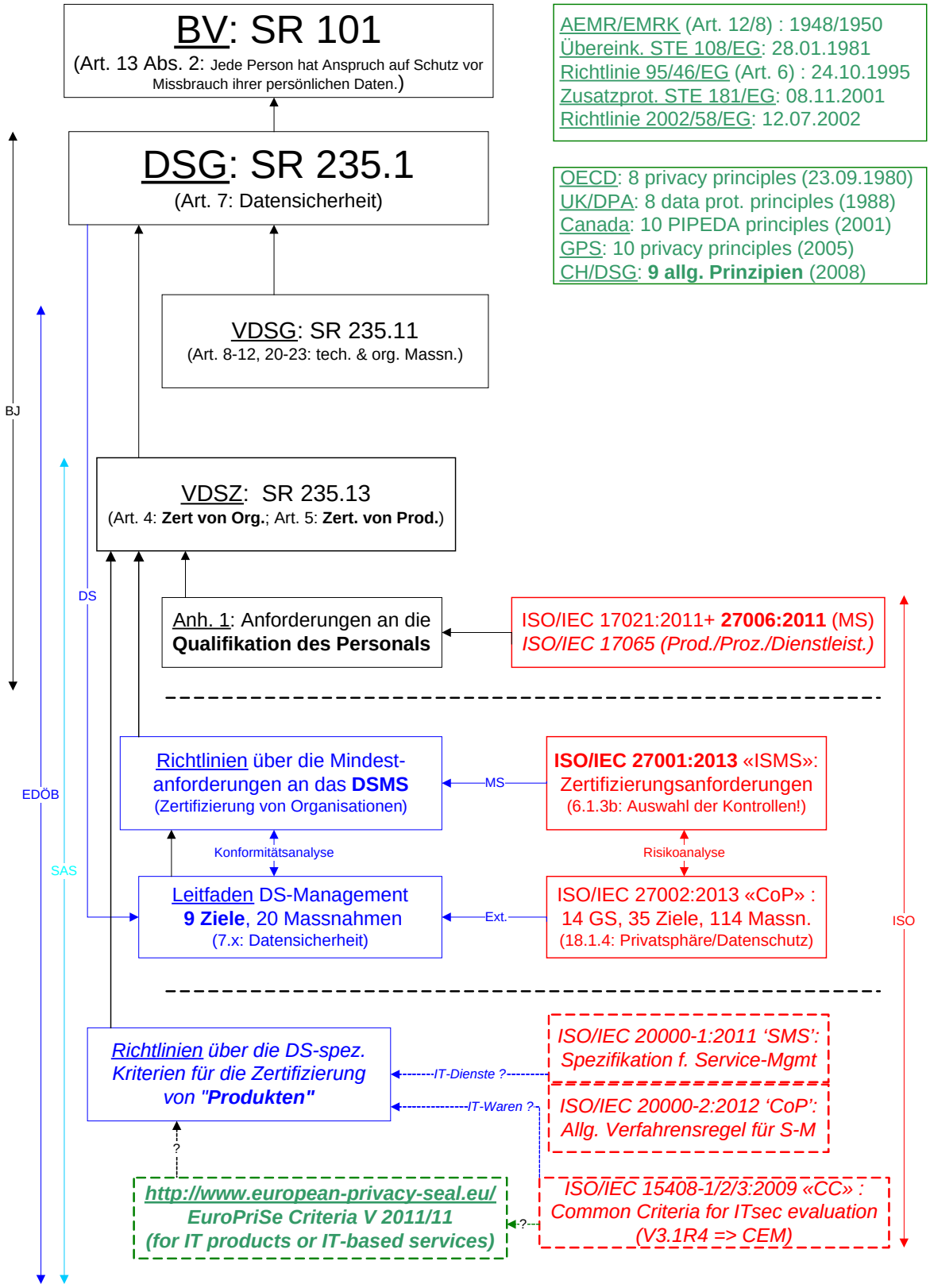
Die dort enthaltenen Schemen auf S. 5 und 2 wurden wie folgt angepasst:




Erwähnenswert im neuen Anhang ist die neue 15. Gruppe über «Lieferantenbeziehungen», deren Ziele (A.15.x) in die DS-Massnahmen a.3 und g.4 betreffend die «Datenbearbeitung durch Dritte» übernommen wurden. Darüber hinaus wurden die Ziele A.6.1.5 über «Informationssicherheit im Projekt-Management» (=>«Privacy by Design») sowie A.6.2 über «Mobilgeräte und Telearbeit» in die DS-Massnahme g.1 zur Datenvertraulichkeit eingefügt.

## Hierarchie der normativen DS-Bestimmungen

EDÖB/PYB/07.04.2014




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)