Zusammenstellung der Ergebnisse der Anhörung zum Entwurf zu Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem

1. Allgemeine Bemerkungen zur Anhörung

Der Bundesrat hat am 28. September 2007 die Inkraftsetzung des revidierten Datenschutzrechts auf den 1. Januar 2008 beschlossen. Die Revision sieht unter anderem die Möglichkeit vor, Datenschutzzertifizierungen durchzuführen. Dafür wurde eine eigene Verordnung (Verordnung über die Datenschutzzertifizierungen [VDSZ]) erlassen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist beauftragt, Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem zu erlassen.
Der Richtlinienentwurf ist für die Praxis, insbesondere für zahlreiche Bereiche der Wirtschaft, bedeutsam. Aus diesem Grund wurde am 31.10.2007 eine Anhörung eröffnet, die bis zum 28. Oktober 2007 dauerte.

28 Organisationen wurden eingeladen, zum Richtlinienentwurf Stellung zu nehmen.

Insgesamt sind acht Stellungnahmen eingegangen (vgl. Auflistung am Schluss).

2. Gegenstand der Anhörung

Gemäss Art. 4 Abs. 3 VDSZ hat der Beauftragte 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 ISO 27001:2005 zu berücksichtigen. Gleichzeitig ist natürlich das Schwergewicht Datenschutz zu wahren.

3. Zusammenfassung der Stellungnahmen zu den wesentlichen Punkten

3.1 Allgemeine Bemerkungen

Der Richtlinienentwurf wird vom Grundsatz her von fünf Organisationen begrüsst (SQS; CLUSIS; SWISS TS; SGS; Datenschutzforum).

Einige Bemerkungen zur Sprache werden von vier Organisationen angebracht (Belser; SWISS TS; SGS; FER).

Eine Organisation (CP) spricht sich dafür aus, dass wer bereits eine Qualitätszertifizierung („certification de qualité“) besitzt, vereinfacht eine DS-Zertifizierung erhalten müsste.

Zwei Organisationen (Belser, Datenschutzforum) weisen darauf hin, dass das DSMS zu kurz komme, und dass der Ansatz, den Begriff Informationssicherheit durch Datenschutz zu ersetzen, dem Datenschutz nicht gerecht werde.

Eine Organisation (Belser) hält weiter fest, dass der EDÖB nicht befugt sei, eine eigene Zertifizierungsnorm zu schaffen.

Dieselbe Organisationen (Belser) vertritt die Ansicht, dass die Hürden für eine DS-Zertifizierung sehr hoch angesetzt seien und daher unattraktiv und unrealistisch. Zwei Organisationen (SQS; FER) halten fest, dass das enge Verhältnis zu ISO 27001 und 27002 subtil gestaltet werden müsse, da sonst die RL den Datenschutz besonders für KMUs erschweren würden. Es sei ein Anforderungskatalog zu erstellen, der auch von KMUs mit verhältnismässigem Aufwand erfüllt werden könne.

Gemäss einer Organisation (FER) sollte der EDÖB die Regeln betreffend geistiges Eigentum (propriété intellectuelle) der Daten in Erinnerung rufen; zudem sei ein Protokoll der Übermittlung von Daten zwischen Staaten nötig.

3.2 Art. 1 Zweck

Mehrere Stellen bemängeln die Tatsache, dass die Richtlinien den Kauf von ISO 27001 voraussetzen würden. So wird vor allem kritisiert, dass die Richtlinien aus sich heraus nicht verständlich seien (Belser; SWISS TS; SGS; Datenschutzforum; Klasse HSLU; FER). SQS verlangt, dass diejenigen Teile des Gesamtumfangs von ISO 27001, die zur Anwendung kommen sollen, aus dem Blickwinkel des DSG genau zu spezifizieren seien.

SWISS TS ist der Auffassung, dass es wichtig sei, die DS-Zertifizierung klar von der ISMS-Zertifizierung zu unterscheiden, denn die Informationssicherheit umfasse ja nur einen Teil des Datenschutzes.

Eine weitere Stelle hält fest, dass die VDSZ auch ISO 9001:2000 erwähne, weshalb es nicht genüge, nur auf ISO 27001:2005 zu verweisen (SGS). Eine andere Stelle erachtet ein alleiniger Verweis auf ISO 27001:2005 als ungenügend, da diese Norm nur die DS-Sicherheit, nicht aber die anderen Datenschutzgrundsätze abdecke, zudem stelle sich die Frage wie bei einer Überarbeitung der Norm vorgegangen würde (Datenschutzforum).

CLUSIS stellt sich die Frage, was in Zusammenhang mit der zukünftigen Norm ISO/CEI 29100 sein wird.

Eine Stelle weist darauf hin, dass eventuelle „Referenzierungen“ als reine Orientierungshilfe zu bezeichnen seien um eine zu technische Ausrichtung zu vermeiden (SQS).

3.3 Art. 2 Auslegung

3.4

Die SGS ist der Auffassung, dass es nicht genügen dürfte, „IS“ einfach in „DS“ umzudeuten. Und auch andere Stellen halten fest, dass Informationssicherheit und Datenschutz nicht dasselbe seien (Datenschutzforum, FER).

3.5 Anhang

Zum Anhang finden sich die verschiedensten Bemerkungen. So hält SWISS TS fest, dass es sinnvoll wäre den Inhalt des Anhangs in die Richtlinien selbst niederzulegen und gleichzeitig weniger stichwortartig zu verfassen. Die SGS und das Datenschutzforum sind der Auffassung, dass klarer darauf hingewiesen werden sollte, dass der Leitfaden eine Hilfe und keine Weisung und nicht abschliessend sei. Das Datenschutzforum findet, es sei darauf hinzuweisen, dass mit dem Leitfaden nur die Datenschutzgrundsätze des 2. Kapitels des DSG abgedeckt seien. Für die SGS und das Datenschutzforum ist zudem fraglich, ob der Begriff „Massnahme“ korrekt verwendet werde. Schliesslich findet Belser, dass es in den Richtlinien keinen Platz für eigene normative Vorschriften habe, zudem sei etwas entweder datenschutzkonform oder nicht.

Organisationen, die Stellungnahmen eingereicht haben:

Belser:	Belser Datenschutz GmbH
SQS	Schweizerische Vereinigung für Qualitäts- und Management-Systeme
CP	Centre Patronal
CLUSIS	Association suisse de la sécurité des systèmes d’information
Swiss TS	Swiss TS Technical Services AG
SGS	SGS Société Générale de Surveillance SA
Datenschutzforum	Datenschutzforum Schweiz
FER	Fédération des Entreprises Romandes