Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Der stellvertretende Beauftragte

Bern, 31.10.2007

An die interessierten Organisationen:

Anhörung: Entwurf zu Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem (Zertifizierung von Organisation und Verfahren)

Sehr geehrte Damen und Herren

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. Diese dienen der Verbesserung des Datenschutzes und der Datensicherheit. Die Durchführung von Zertifizierungen bleibt vollumfänglich privaten Zertifizierungsstellen überlassen. Da es sich um eine vollständig neue Materie handelt, wurde dafür eine eigene Verordnung (Verordnung über die Datenschutzzertifizierungen [VDSZ]) erlassen.

Das revidierte Gesetz sieht folgende zwei Zertifizierungsobjekte vor: die Zertifizierung von Organisation und Verfahren des Datenschutzes (Datenschutzmanagementsystem) einerseits und die Zertifizierung von Produkten andererseits (Programme und Systeme) andererseits. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist beauftragt, zunächst Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem und sodann – bis spätestens am 1. Januar 2010 – Richtlinien darüber, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind, zu erlassen. Der EDÖB wird mit dem Erlass der Richtlinien betreffend die Zertifizierung von Produkten etwas zuwarten, um die zur Zeit auf europäischer Ebene in diesem Bereich laufenden Bestrebungen zur Erarbeitung von standardisierten Vorgaben beobachten zu können.

Gemäss Artikel 4 Abs. 3 VDSZ erlässt der oder die Beauftragte Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem. Er oder sie berücksichtigt dabei internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere die Normen ISO 27001:2005. Vorliegend handelt es sich um einen Entwurf von Richtlinien, die für die Praxis, insbesondere für zahlreiche Bereiche der Wirtschaft bedeutsam sind. Aus diesem Grund führen wir eine Anhörung nach Artikel 10 Vernehmlassungsgesetz (SR 172.061) durch. Wir unterbreiten Ihnen daher den Entwurf der Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem mit dem Anhang und den Erläuterungen zur Stellungnahme.

Die vorliegenden Richtlinien stützen sich hauptsächlich auf **ISO/IEC 27001:2005**, legen aber das Schwergewicht auf den Datenschutz. So geht es vor allem darum, „Informationssicherheit“ durch Datenschutz zu ersetzen, und „Risikomanagement“ mit „Konformitätsmanagement“ zu ergänzen. Die allgemeinen Voraussetzungen für Managementsysteme wurden von ISO 27001 übernommen. Um die Ausrichtung zum normativen Anhang A – bestehend aus den direkt der Norm **ISO/IEC 27002:2005** entzogenen Zielen und Sicherheitsmassnahmen – beizubehalten, enthalten die Richtlinien als Anhang einen Umsetzungsleitfaden, bestehend aus 20 Massnahmen, die die 9 Datenschutzgrundsätze konkretisieren.

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

Wir bitten Sie, Ihre Stellungnahmen bis zum **28. November 2007** direkt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, 3003 Bern, auf schriftlichem Weg zukommen zu lassen. Für allfällige Fragen stehen Ihnen Herr Pierre-Yves Baumann (031 322 43 48; pierre-yves.baumann@edoeb.admin.ch) oder Frau Caroline Gloor Scheidegger (031 322 47 52 caroline.gloorscheidegger@edoeb.admin.ch) gerne zur Verfügung. Zusätzliche Exemplare der Anhörungsunterlagen können über die Internetadresse www.edoeb.ch – *Themen – Datenschutz – sonstige Themen – Revision des Bundesgesetzes über den Datenschutz DSG* bezogen werden. Die Unterlagen können Sie auch beim Sekretariat des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Tel. 031 322 43 95, Mo. bis Fr., 10.00 bis 12.00 Uhr) bestellen.

Mit freundlichen Grüssen

Jean-Philippe Walter

Beilagen:
- Richtlinienentwurf mit Anhang und Erläuterungen
- Liste der begrüssten Organisationen