Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem

(Richtlinien über die Zertifizierung von Organisation und Verfahren)

vom 16. Juli 2008

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte,

gestützt auf Artikel 11 Absatz 2 des Bundesgesetzes vom 19. Juni 1992[1] über den Datenschutz (DSG)
und auf Artikel 4 Absatz 3 der Verordnung vom 28. September 2007[2] über die Datenschutzzertifizierungen (VDSZ),

erlässt folgende Richtlinien:

1. Zweck

1 Diese Richtlinien legen die Mindestanforderungen fest, die ein Datenschutzmanagementsystem (DSMS) erfüllen muss, damit Organisation und Verfahren nach Artikel 4 VDSZ zertifiziert werden können.

2 Sie bezwecken, ein Modell für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines DSMS zu liefern.

3 Sie decken alle Organisationsarten ab.

2. Definitionen

Zusätzlich zu den Definitionen der Kapitel 3.1–3.16 der Norm ISO/IEC 27001:2005[3] bedeuten die folgenden Ausdrücke:

a. *Konformitätsmanagement:* koordinierte Tätigkeiten einer Organisation mit dem Ziel, die für sie geltenden gesetzlichen und reglementarischen Voraussetzungen, insbesondere diejenigen betreffend Datenschutz, einzuhalten;

b. *Beurteilung der Nichtkonformität:* gesamter Prozess der Analyse und der Bewertung der Nichtkonformität;

c. *Analyse der Nichtkonformität:* die systematische Auswertung von Informationen mit dem Ziel, die Ursachen der Nichtkonformität zu identifizieren und die Nichtkonformität einzuschätzen;

1 SR **235.1**
2 SR **235.13**
3 «Informationssicherheits-Managementsysteme – Anforderungen», unter Lizenz auf Papier oder als PDF erhältlich bei www.iso.org.

d. *Bewertung der Nichtkonformität:* Prozess, in dem die eingeschätzte Nichtkonformität mit den festgelegten Kriterien verglichen wird, um die Bedeutung der Nichtkonformität zu bestimmen (leichte oder erhebliche Nichtkonformität);

e. *Behandlung der Nichtkonformität:* Verfahren zur Auswahl und Umsetzung von Massnahmen zur Beseitigung einer Nichtkonformität[4].

3. Realisierung

[1] Ein DSMS genügt den Mindestanforderungen, wenn es die bestehenden internationalen Normen erfüllt, insbesondere die Norm ISO 27001, die nach Absatz 2 auszulegen und im Sinne von Abschnitt 4 zu ergänzen oder abzuändern ist.

[2] Die Anforderungen der Norm ISO 27001 betreffend das Informationssicherheitsmanagementsystem (ISMS) sind wie folgt zu übernehmen: Einerseits ist anstelle des Begriffs Informationssicherheit (IS) der Begriff Datenschutz (DS) einzusetzen, andererseits ist Anhang A der Norm ISO 27001, der dem Inhaltsverzeichnis der Norm ISO/IEC 27002:2005[5] entspricht, durch die in Abschnitt 5 aufgeführten Ziele und Massnahmen zu ersetzen.

4. Umsetzung (Mindestanforderungen)

Das durch die Organisation aufgestellte DSMS muss mindestens die in der Norm ISO 27001 aufgeführten Mindestanforderungen enthalten und gleichzeitig die folgenden datenschutzrechtlichen Aspekte berücksichtigen:

a. Generell gilt, dass der Begriff der (Nicht-)Konformität in Bezug auf die Datenschutzvoraussetzungen systematisch denjenigen der Informationssicherheitsrisiken ergänzt. Somit ergänzt die Konformitätsanalyse die in der Norm ISO 27001 vorgesehene Risikoanalyse, wobei jede Nichtkonformität auszuschliessen ist.

b. Spezifisch sind bei der Erstellung eines DSMS die folgenden Ziffern der Norm ISO 27001 wie folgt auszulegen:

   4.2.1. a. Der Anwendungsbereich und die Grenzen des DSMS sind nach Artikel 4 Absatz 1 VDSZ zu definieren;

   4.2.1. b. Die DSMS-Leitlinie entspricht der Datenschutzpolitik nach Artikel 4 Absatz 2 Buchstabe a VDSZ;

4 Alternativ kann eine Nichtkonformität auch vermieden werden, indem beispielsweise auf die betreffende Bearbeitung verzichtet wird. Eine Nichtkonformität darf hingegen weder akzeptiert noch übertragen werden.

5 «Leitfaden für das Informationssicherheits-Management», unter Lizenz auf Papier oder als PDF erhältlich bei www.iso.org.

4.2.1. d 1. Insbesondere sind die Werte der Art Datensammlungen (Art. 3 Bst. g DSG) und deren Eigentümer, vorliegend also der Daten inhaber (Art. 3 Bst. i DSG), zu bestimmen;

4.2.1. g. Die in Abschnitt 5 aufgeführten eigentlichen Datenschutzziele und -massnahmen sind als Bestandteil dieses Prozesses auszuwählen, insoweit sie diese Anforderungen erfüllen können;

4.3.1. j[6]. Die Dokumentation des DSMS muss mindestens die Liste der nicht angemeldeten Datensammlungen (vgl. Abschnitt 5 Buchstabe h Ziffer 2) beinhalten.

5. Ziele und Massnahmen

Bei der Erstellung des DSMS müssen folgende Ziele und Massnahmen[7] erfüllt sein:

a. Rechtmässigkeit (Art. 4 Abs. 1 DSG)
   1. Rechtfertigungsgründe (Art. 13 DSG)
   2. Gesetzliche Grundlage (Art. 17, 19 und 20 DSG)
   3. Datenbearbeitung durch Dritte (Art. 10*a* Abs. 1 DSG)

b. Transparenz
   1. Treu und Glauben (Art. 4 Abs. 2 DSG)
   2. Erkennbarkeit (Art. 4 Abs. 4 DSG)
   3. Informationspflicht (Art. 7*a* Abs. 1 DSG)

c. Verhältnismässigkeit
   1. Verhältnismässige Bearbeitung (Art. 4 Abs. 2 DSG)

d. Zweckbindung (Art. 4 Abs. 3 DSG)
   1. Zweckbestimmung / Zweckänderung (Art. 3 Bst. i DSG)
   2. Nutzungsbeschränkung

e. Datenrichtigkeit
   1. Datenrichtigkeit (Art. 5 Abs. 1 DSG)
   2. Berichtigung von Daten (Art. 5 Abs. 2 DSG)

f. Grenzüberschreitende Datenbekanntgabe (Art. 6 Abs. 1 DSG)
   1. Angemessener Schutz (Art. 6 Abs. 2 DSG)

6 Zusätzlicher Buchstabe zur Norm ISO 27001.

7 Die aufgeführten Ziele und Massnahmen stammen aus dem «Leitfaden für das Datenschutz-Management» (der Text kann unter www.edoeb.admin.ch eingesehen werden) und wurden entsprechend übernommen. Der Massnahmenkatalog ist nicht abschliessend und einer Organisation ist es freigestellt, zusätzliche Ziele oder Massnahmen zu berücksichtigen. Die Ziele und Massnahmen dieses Katalogs müssen bei der Durchführung des DSMS als Bestandteil des Prozesses ausgewählt werden. Der «Leitfaden für das Datenschutz-Management» enthält Umsetzungsempfehlungen und Leitlinien betreffend die besten Praktiken und dient als Unterstützung der vorgeschlagenen Massnahmen. Dieser Leitfaden entspricht der Norm ISO 27002 («Leitfaden für das Informationssicherheits-Management»). Die 9 ausgewählten Ziele entstammen direkt aus dem DSG und die 20 dazugehörigen Massnahmen sind analog zur Norm ISO 27002 strukturiert.

g. Datensicherheit (Art. 7 DSG)
   1. Datenvertraulichkeit
   2. Datenintegrität
   3. Datenverfügbarkeit
   4. Datenbearbeitung durch Dritte (Art 10*a* Abs. 2 DSG)

h. Registrierung der Datensammlungen (Art. 11*a* Abs. 1 DSG und Art. 12*b* Abs. 1 VDSG)
   1. Anmeldepflicht (Art. 11*a* Abs. 2 et 3; Ausnahmen Art. 11*a* Abs. 5 Bst. e und f DSG)
   2. Liste der nicht angemeldeten Datensammlungen (Art. 12*b* Abs. 1 Bst. b VDSG)

i. Auskunftsrecht und Verfahren
   1. Auskunftsrecht betreffend eigene Daten (Art. 8 Abs. 1 DSG)
   2. Rechtsansprüche und Verfahren (Art. 15 und 25 DSG)

6. Inkrafttreten

Diese Richtlinien treten am 1. September 2008 in Kraft.

16. Juli 2008

Eidgenössischer
Datenschutz- und Öffentlichkeitsbeauftragter:

Hanspeter Thür