Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem

(Richtlinien über die Zertifizierung von Organisation und Verfahren)

vom 19. März 2014

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 Begriffen und Definitionen der Ziffern 2.1–2.89 der Norm ISO/IEC 27000:2014[3] bedeuten die folgenden Ausdrücke:

a. *Konformitätsmanagement:* koordinierte Tätigkeiten, um eine Organisation in Bezug auf die Konformität zu steuern und zu überwachen, insbesondere diejenigen betreffend Datenschutz;

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

c. *Analyse der Nichtkonformität:* Verfahren, um die Art der Nichtkonformität zu verstehen und um die Nichtkonformitätsstufe (ausgedrückt als Verhältnis zwischen den Auswirkungen und ihrer Eintretenswahrscheinlichkeit) zu bestimmen;

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

d. *Bewertung der Nichtkonformität:* Verfahren zum Vergleich der Ergebnisse der Analyse der Nichtkonformität mit den Konformitätskriterien, um zu bestimmen, ob die Nichtkonformität oder deren Bedeutung vertretbar ist;

e. *Behandlung der Nichtkonformität:* Verfahren zur Änderung (Milderung, Entfernung, Vorbeugung, Verminderung oder Vermeidung, nicht aber zur Akzeptierung, Teilung oder Übertragung) der Nichtkonformität.

3. Realisierung

1 Ein DSMS genügt den Mindestanforderungen, wenn es die bestehenden internationalen Normen erfüllt, insbesondere die Norm ISO/IEC 27001:2013[4], die nach Absatz 2 auszulegen und im Sinne von Ziffer 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 27002:2013[5] entspricht, durch die unter Ziffer 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 verbleibende Nichtkonformität auszuschliessen ist.

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

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

   5.2. Die Datenschutzleitlinie[6] entspricht der Datenschutzpolitik nach Artikel 4 Absatz 2 Buchstabe a VDSZ.

4 «Informationssicherheits-Managementsysteme – Anforderungen», unter Lizenz auf Papier oder als PDF / ePub erhältlich bei www.iso.org.

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

6 Diese übergeordnete Datenschutzleitlinie wird durch andere thematische Leitlinien zur Informationssicherheit oder zum Privatsphärenschutz (Beschreibung in der Massnahme A.5.1.1) ergänzt.

6.1.2. c.2. Insbesondere sind die Werte der Art Datensammlungen (Art. 3 Bst. g DSG) und deren Eigentümer, vorliegend der Dateninhaber (Art. 3 Bst. i DSG), zu bestimmen.

6.1.3. b. Die unter Ziffer 5 aufgeführten eigentlichen Datenschutzziele und -massnahmen sind als Bestandteil dieses Prozesses auszuwählen, soweit sie diese Anforderungen erfüllen können.

7.5.1. c.[7] Die Dokumentation des DSMS muss mindestens die Liste der nicht angemeldeten Datensammlungen (vgl. Ziff. 5 Bst. h Ziff. 2) beinhalten.

5. Ziele und Massnahmen

Bei der Erstellung des DSMS müssen folgende Ziele und Massnahmen[8] 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);

7 Zusätzlicher Buchstabe zur Norm ISO 27001.

8 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. Entsprechend der Norm ISO 27002, enthält der «Leitfaden für das Datenschutz-Management» Umsetzungsempfehlungen und Leitlinien betreffend die besten Praktiken und dient als Unterstützung der vorgeschlagenen Massnahmen. Die neun ausgewählten Ziele entstammen direkt aus dem DSG und die 20 dazugehörigen Massnahmen sind analog zur Norm ISO 27002 strukturiert.

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

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 und 3 DSG; 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. Aufhebung eines anderen Erlasses

Die Richtlinien vom 16. Juli 2008[9] über die Mindestanforderungen an ein Datenschutzmanagementsystem werden aufgehoben.

7. Übergangsbestimmung

Für Zertifizierungsverfahren, die zum Zeitpunkt des Inkrafttretens dieser Richtlinien hängig sind, gilt das bisherige Recht. Diese Zertifizierungsverfahren müssen bis zum 1. Oktober 2014 abgeschlossen sein.

8. Inkrafttreten

Diese Richtlinien treten am 1. Mai 2014 in Kraft.

19. März 2014

Eidgenössischer
Datenschutz- und Öffentlichkeitsbeauftragter:

Hanspeter Thür

9 BBl **2008** 7237