Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Richtlinien über die Mindestanforderungen an ein Managementsystem

(Richtlinien über die Zertifizierung von Managementsystemen)

vom 31. August 2023

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte,

gestützt auf Artikel 6 Absatz 2 der Verordnung vom 31. August 2022[1] über die Datenschutzzertifizierungen (VDSZ),

erlässt folgende Richtlinien:

1. Zweck

[1] Diese Richtlinien legen die Mindestanforderungen fest, die ein Managementsystem (MS) erfüllen muss, damit Organisation und Verfahren nach Artikel 6 VDSZ zertifiziert werden können.

[2] Sie bezwecken, ein Modell für die Errichtung, den Betrieb, die Überwachung, Überprüfung, Instandhaltung und Verbesserung eines MS zu liefern.

[3] Sie decken alle Organisationsarten ab.

2. Definitionen

Zusätzlich zu den Begriffen und Definitionen der Norm ISO/IEC 27000[2] 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;

1 SR **235.13**

2 «Information security management systems – Overview and vocabulary», unter Lizenz auf Papier oder als PDF erhältlich bei www.iso.org. Die aufgeführten Normen können kostenlos eingesehen und gegen Bezahlung bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch

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;

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 MS genügt den Mindestanforderungen, wenn es die bestehenden internationalen Normen erfüllt, insbesondere die Norm ISO/IEC 27001[3], die nach Absatz 2 auszulegen und im Sinne von Ziffer 4 zu ergänzen oder abzuändern ist.

2 Die Anforderungen der Norm ISO/IEC 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/IEC 27001, der dem Inhaltsverzeichnis der Norm ISO/IEC 27002[4] entspricht, durch die unter Ziffer 5 aufgeführten Ziele und Massnahmen zu ergänzen.

4. Umsetzung (Mindestanforderungen)

Das durch die Organisation aufgestellte MS muss mindestens die in der Norm ISO/IEC 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/IEC 27001 vorgesehene Risikoanalyse, wobei jede verbleibende Nichtkonformität auszuschliessen ist.

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

4.3. Der Anwendungsbereich und die Grenzen des MS sind nach Artikel 4 Absatz 2 VDSZ zu definieren.

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

4 «Information security controls», unter Lizenz auf Papier oder als PDF / ePub erhältlich bei www.iso.org.

5.2. Die Datenschutzleitlinie[5] entspricht der Datenschutzpolitik nach Artikel 6 Absatz 1 Buchstabe a VDSZ.

6.1.2. c.2. Insbesondere sind die Werte der Art Bearbeitungstätigkeiten (Art. 5 Bst. d und Art. 12 DSG) und deren Verantwortliche (Risikoeigentümer) (Art. 5 Bst. j 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.[6] Die Dokumentation des MS muss mindestens das Verzeichnis der Bearbeitungstätigkeiten und eine Beurteilung ob die Bearbeitungstätigkeiten hohe Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge haben, beinhalten.

5. Ziele und Massnahmen

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

a. Rechtmässigkeit (Art. 6 Abs. 1 DSG):
   1. Rechtfertigungsgründe (Art. 31 DSG),
   2. Gesetzliche Grundlage (Art. 34 und 36 DSG),
   3. Datenbearbeitung durch Auftragsbearbeiter (Art. 9 DSG i.V.m. Art. 7 DSV);

b. Transparenz:
   1. Treu und Glauben (Art. 6 Abs. 2 DSG),
   2. Erkennbarkeit (Art. 6 Abs. 3 DSG),
   3. Informationspflicht (Art. 19 – 21 DSG i.V.m. Art. 13 DSV),
   4. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG i.V.m. Art. 24 DSV),
   5. Datenschutz-Folgenabschätzung (Art. 22 DSG i.V.m. Art. 14 DSV),
   6. Meldung von Verletzungen der Datensicherheit (Art. 24 DSG i.V.m. Art. 15 DSV);

c. Verhältnismässigkeit:
   1. Verhältnismässige Bearbeitung (Art. 6 Abs. 2 DSG),
   2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 7 DSG);

5 Diese übergeordnete Datenschutzleitlinie wird durch andere thematische Leitlinien zur Informationssicherheit oder zum Privatsphärenschutz (Beschreibung in der Massnahme A.5.1) ergänzt.

6 Zusätzlicher Buchstabe zur Norm ISO/IEC 27001.

7 Die aufgeführten Ziele und Massnahmen sind 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 MS als Bestandteil des Prozesses ausgewählt werden.

d. Zweckbindung (Art. 6 Abs. 3 DSG);

e. Datenrichtigkeit (Art. 6 Abs. 5 DSG);

f. Bekanntgabe von Personendaten ins Ausland (Art. 16 DSG i.V.m. Art. 8 – 12 DSV);

g. Datensicherheit (Art. 8 DSG i.V.m. Art. 1 – 6 DSV);

h. Rechte und Verfahren:

1. Auskunftsrecht über eine Person betreffende Daten (Art. 25 DSG i.V.m. Art. 16 – 19 DSV),

2. Recht auf Datenherausgabe oder -übertragung (Art. 28 DSG i.V.m. Art. 20 – 22 DSV),

3. Rechtsansprüche und Verfahren (Art. 32 und 41f. DSG).

6. Aufhebung eines anderen Erlasses

Die Richtlinien vom 19. März 2014[8] 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. März 2024 abgeschlossen sein.[9]

8. Inkrafttreten

Diese Richtlinien treten am 1. September 2023 in Kraft.

31. August 2023

Eidgenössischer
Datenschutz- und Öffentlichkeitsbeauftragter:

Adrian Lobsiger

8 BBl **2014** 3137

9 Die weiteren Übergangsbestimmungen werden von der Schweizerische Akkreditierungsstelle (SAS) publiziert.