Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Richtlinien über die weiteren datenschutzrechtlichen Kriterien für die Prüfung zu den Anforderungen an die Zertifizierung von Produkten, Dienstleistungen und Prozessen

vom 31. August 2023

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte,

gestützt auf Artikel 7 Absatz 2 der Verordnung vom 31. August 2022[1] über die Datenschutzzertifizierungen (VDSZ),

erlässt folgende Richtlinien:

1. Zweck

[1] Diese Richtlinien legen die weiteren datenschutzrechtlichen Kriterien für die Prüfung zu den Anforderungen an die Zertifizierung von Produkten, Dienstleistungen und Prozessen fest, damit Produkte, Dienstleistungen und Prozesse nach Artikel 7 VDSZ zertifiziert werden können.

[2] Sie bezwecken, die Grundsätze nach Artikel 6 DSG und weitere Forderungen aus dem DSG und der DSV aufzuzeigen.

[3] Sie stellen sicher, dass die zertifizierten Produkte, Dienstleistungen und Prozessen die Vorgaben nach Artikel 7 Absatz 1 VDSZ einhalten.

2. Ziele und Massnahmen

Bei der Erstellung des Zertifizierungsprogramm müssen neben den Anforderungen von Artikel 5 und 7 VDSZ folgende Ziele und Massnahmen[2] erfüllt sein:

a. Rechtmässigkeit (Art. 6 Abs. 1 DSG):
   1. Rechtfertigungsgründe (Art. 31 DSG),
   2. Gesetzliche Grundlage (Art. 34 und 36 DSG),

1 SR **235.13**
2 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 Zertifizierungsprogramm als Bestandteil des Prozesses ausgewählt werden.

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);

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).

3. 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.[3]

[3] Die weiteren Übergangsbestimmungen werden von der Schweizerische Akkreditierungsstelle (SAS) publiziert.

4. Inkrafttreten

Diese Richtlinien treten am 1. September 2023 in Kraft.

31. August 2023

Eidgenössischer
Datenschutz- und Öffentlichkeitsbeauftragter:

Adrian Lobsiger