Verordnung über Datenschutzzertifizierungen (VDSZ)

vom 31. August 2022

Der Schweizerische Bundesrat,

gestützt auf Artikel 13 Absatz 2 des Datenschutzgesetzes vom 25. September 2020[1] (DSG),

verordnet:

1. Abschnitt: Zertifizierungsstellen

Art. 1 Anforderungen

[1] Stellen, die Datenschutzzertifizierungen nach Artikel 13 DSG durchführen (Zertifizierungsstellen), müssen akkreditiert sein. Die Akkreditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[2] (AkkBV), soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

[2] Je eine separate Akkreditierung ist erforderlich für die Zertifizierung:

a. der Organisation und der Verfahren (Managementsysteme) im Zusammenhang mit Datenbearbeitungen;

b. von Produkten, namentlich Datenbearbeitungssystemen oder -programmen und Hardware, sowie von Dienstleistungen und Prozessen im Zusammenhang mit Datenbearbeitungen.

[3] Die Zertifizierungsstellen müssen über eine festgelegte Organisation sowie ein festgelegtes Zertifizierungsverfahren (Zertifizierungsprogramm) verfügen.

[4] Die Mindestanforderungen an die Qualifikation des Personals, das Zertifizierungen durchführt, richten sich nach dem Anhang. Die Zertifizierungsstellen müssen nachweisen, dass sie über entsprechend diesen Kriterien qualifiziertes Personal verfügen.

Art. 2 Akkreditierungsverfahren

Die Schweizerische Akkreditierungsstelle (SAS) zieht für das Akkreditierungsverfahren und die Nachkontrolle sowie für die Sistierung oder den Entzug einer Akkreditierung den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei.

SR **235.13**

1 SR **235.1**

2 SR **946.512**

Art. 3 Ausländische Zertifizierungsstellen

[1] Ausländische Zertifizierungsstellen, die auf schweizerischem Territorium tätig sein wollen, müssen nachweisen, dass sie über eine gleichwertige Qualifikation verfügen und die Anforderungen nach Artikel 1 Absätze 3 und 4 erfüllen sowie dass ihnen die schweizerische Datenschutzgesetzgebung hinreichend bekannt ist.

[2] Der EDÖB anerkennt eine ausländische Zertifizierungsstelle nach Rücksprache mit der SAS.

[3] Er kann die Anerkennung befristen und mit Auflagen verbinden.

[4] Er entzieht die Anerkennung, wenn die Bedingungen und Auflagen nicht mehr erfüllt sind.

2. Abschnitt: Gegenstand und Verfahren

Art. 4 Gegenstand der Zertifizierung

[1] Zertifizierbar sind:

a. Managementsysteme;

b. Produkte, Dienstleistungen und Prozesse.

[2] Die Zertifizierung von Managementsystemen kann die Gesamtheit des Systems, einzelne Teile der Organisation oder einzelne, abgrenzbare Verfahren umfassen.

[3] Die Zertifizierung von Produkten, Dienstleistungen und Prozessen kann Folgendes umfassen:

a. Produkte, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten erzeugt werden;

b. Dienstleistungen oder Prozesse, die hauptsächlich der Bearbeitung von Personendaten dienen oder die Personendaten erzeugen.

Art. 5 Anforderungen an das Zertifizierungsprogramm

[1] Im Zertifizierungsprogramm müssen mindestens geregelt sein:

a. die Prüfkriterien und die sich daraus ergebenden Anforderungen an die zu zertifizierenden Gegenstände;

b. der Ablauf des Verfahrens, insbesondere das Vorgehen, wenn Unregelmässigkeiten festgestellt werden.

[2] Bei der Festlegung des Zertifizierungsprogramms muss Folgendes berücksichtigt werden:

a. die zu bearbeitenden Personendaten;

b. die für die Bearbeitung der Personendaten verwendete elektronische Infrastruktur;

c. die organisatorischen Massnahmen im Zusammenhang mit der Bearbeitung von Personendaten.

[3] Die Prüfkriterien müssen mit allen Grundsätzen nach Artikel 6 DSG übereinstimmen.

[4] Das Zertifizierungsprogramm muss den gemäss Anhang 2 AkkBV[3] anwendbaren Normen sowie weiteren anwendbaren technischen Normen entsprechen.

Art. 6 Anforderungen an die Zertifizierung von Managementsystemen

[1] Gegenstand der Prüfung von Managementsystemen sind insbesondere:

a. die Datenschutzpolitik;

b. die Dokumentation von Zielen, Risiken und Massnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit;

c. die organisatorischen und technischen Vorkehrungen zur Umsetzung der festgelegten Ziele und Massnahmen, insbesondere zur Behebung von Mängeln.

[2] Der EDÖB erlässt Richtlinien über die Mindestanforderungen an das Managementsystem. Er berücksichtigt dabei die internationalen Anforderungen an die Errichtung, den Betrieb, die Überwachung und die Verbesserung solcher Managementsysteme und insbesondere die folgenden technischen Normen[4]:

a. SN EN ISO 9001, Qualitätsmanagementsysteme, Anforderungen;

b. SN EN ISO/IEC 27001, Informationstechnik, IT-Sicherheitsverfahren, Informationssicherheits-Managementsysteme, Anforderungen;

c. SN EN ISO/IEC 27701, IT-Sicherheitsverfahren, Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Schutz der Privatsphäre, Anforderungen und Richtlinien.

Art. 7 Anforderungen an die Zertifizierung von Produkten, Dienstleistungen und Prozessen

[1] Gegenstand der Prüfung von Produkten, Dienstleistungen und Prozessen ist insbesondere die Gewährleistung:

a. der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der bearbeiteten Personendaten;

b. der Vermeidung der Bearbeitung von Personendaten, die im Hinblick auf den Verwendungszweck des Produkts, der Dienstleistung oder des Prozesses nicht erforderlich sind;

c. der Transparenz der Bearbeitung von Personendaten;

3 SR **946.512**

4 Die aufgeführten Normen können kostenlos eingesehen und gegen Bezahlung bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.

d. von technischen Massnahmen zur Unterstützung der Anwenderin oder des Anwenders bei der Einhaltung weiterer Datenschutzgrundsätze und datenschutzrechtlicher Pflichten, insbesondere der Rechte der betroffenen Personen.

[2] Der EDÖB erlässt Richtlinien darüber, nach welchen weiteren datenschutzrechtlichen Kriterien die Prüfung erfolgen muss.

Art. 8 Erteilung und Gültigkeit der Datenschutzzertifizierung

[1] Die Zertifizierungsstelle zertifiziert das Managementsystem, das Produkt, die Dienstleistung oder den Prozess, wenn die datenschutzrechtlichen Anforderungen und die Voraussetzungen nach dieser Verordnung, nach den vom EDÖB erlassenen Richtlinien oder nach anderen gleichwertigen Normen erfüllt sind. Die Zertifizierung kann mit Auflagen verbunden werden.

[2] Die Zertifizierung ist drei Jahre gültig. Die Zertifizierungsstelle muss jährlich prüfen, ob die Voraussetzungen weiterhin erfüllt sind.

Art. 9 Anerkennung ausländischer Datenschutzzertifizierungen

Der EDÖB anerkennt nach Rücksprache mit der SAS ausländische Zertifizierungen, wenn gewährleistet ist, dass die Anforderungen der schweizerischen Gesetzgebung erfüllt sind.

Art. 10 Ausnahme von der Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung

Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung gemäss Artikel 22 Absatz 5 DSG nur absehen, wenn die Zertifizierung die Bearbeitung, die im Rahmen der Datenschutz-Folgenabschätzung zu prüfen wäre, einschliesst.

3. Abschnitt: Sanktionen

Art. 11 Sistierung und Entzug der Zertifizierung

[1] Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, insbesondere wenn sie im Rahmen der Überprüfung schwere Mängel feststellt. Ein schwerer Mangel liegt insbesondere vor, wenn:

a. wesentliche Voraussetzungen der Datenschutzzertifizierung nicht mehr erfüllt sind; oder

b. eine Zertifizierung irreführend oder missbräuchlich verwendet wird.

[2] Bei Streitigkeiten über die Sistierung oder den Entzug richten sich die Beurteilung und das Verfahren nach den zivilrechtlichen Bestimmungen, die auf das Vertragsver-

hältnis zwischen der Zertifizierungsstelle und dem Hersteller von Datenbearbeitungssystemen oder -programmen, dem Verantwortlichen oder dem Auftragsbearbeiter, der die Zertifizierung erhalten hat, anwendbar sind.

Art. 12 Verfahren bei Aufsichtsmassnahmen des EDÖB

[1] Stellt der EDÖB bei einem Hersteller von Datenbearbeitungssystemen oder -programmen, einem Verantwortlichen oder einem Auftragsbearbeiter, der über eine Zertifizierung verfügt, schwere Mängel fest, so informiert er die Zertifizierungsstelle darüber.

[2] Die Zertifizierungsstelle fordert den Hersteller von Datenbearbeitungssystemen oder -programmen, den Verantwortlichen oder den Auftragsbearbeiter unverzüglich auf, den Mangel innerhalb von 30 Tagen, nachdem sie vom EDÖB informiert wurde, zu beheben.

[3] Wird der Mangel nicht innerhalb von 30 Tagen behoben, so sistiert die Zertifizierungsstelle die Zertifizierung. Besteht keine Aussicht darauf, dass innerhalb eines angemessenen Zeitraums ein rechtskonformer Zustand geschaffen oder wiederhergestellt wird, so wird die Zertifizierung entzogen.

[4] Wird der Mangel nicht innerhalb der Frist nach Absatz 2 behoben und hat die Zertifizierungsstelle die Zertifizierung nicht sistiert oder entzogen, so trifft der EDÖB eine Massnahme nach Artikel 51 Absatz 1 DSG. Er kann namentlich anordnen, die Zertifizierung zu sistieren oder zu entziehen. Richtet er die Verfügung an die Zertifizierungsstelle, so informiert er die SAS darüber.

4. Abschnitt: Schlussbestimmungen

Art. 13 Aufhebung eines anderen Erlasses

Die Verordnung über die Datenschutzzertifizierungen vom 28. September 2007[5] wird aufgehoben.

Art. 14 Inkrafttreten

Diese Verordnung tritt am 1. September 2023 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ignazio Cassis
Der Bundeskanzler: Walter Thurnherr

5 AS **2007** 5003, **2010** 949, **2016** 3447

Anhang
(Art. 1 Abs. 4)

Mindestanforderungen an die Qualifikation des Personals

1 Zertifizierung von Managementsystemen

Das Personal, das Managementsysteme zertifiziert, muss gesamthaft über folgende Qualifikationen verfügen:

- Kenntnisse im Bereich des Datenschutzrechts: mindestens zweijährige praktische Tätigkeit im Bereich des Datenschutzes oder erfolgreich abgeschlossene, mindestens einjährige Ausbildung an einer Hochschule oder Fachhochschule mit Schwerpunkt Datenschutzrecht;
- Kenntnisse im Bereich der Informationssicherheit: mindestens zweijährige praktische Tätigkeit im Bereich der Informationssicherheit oder erfolgreich abgeschlossene, mindestens einjährige Ausbildung an einer Hochschule oder Fachhochschule mit Schwerpunkt Informationssicherheit;
- Kenntnisse der Entwicklungen im Bereich des Datenschutzrechts und im Bereich der Informationssicherheit;
- Ausbildung als Auditorin oder Auditor von Managementsystemen, die insbesondere die international massgebenden Anforderungen der folgenden Normen[6] erfüllt:
  - SN EN ISO/IEC 17021-1, Konformitätsbewertung, Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, Teil 1: Anforderungen,
  - SN EN ISO/IEC 17021-3, Konformitätsbewertung, Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, Teil 3: Anforderungen an die Kompetenz für die Auditierung und Zertifizierung von Qualitätsmanagementsystemen, und
  - SN EN ISO/IEC 27006, Informationstechnik, IT-Sicherheitsverfahren, Anforderungen an Institutionen, die Audits und Zertifizierung von Informationssicherheits-Managementsystemen anbieten.

Die Zertifizierungsstelle muss für die einzelnen Bereiche über qualifiziertes Personal verfügen. Die Prüfung der Managementsysteme durch ein interdisziplinäres Team ist zulässig.

2 Zertifizierung von Produkten, Dienstleistungen und Prozessen

Das Personal, das Produkte, Dienstleistungen oder Prozesse zertifiziert, muss gesamthaft über folgende Qualifikationen verfügen:

6 Die aufgeführten Normen können kostenlos eingesehen und gegen Bezahlung bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.

- Kenntnisse im Bereich des Datenschutzrechts: mindestens zweijährige praktische Tätigkeit im Bereich des Datenschutzes oder erfolgreich abgeschlossene, mindestens einjährige Ausbildung an einer Hochschule oder Fachhochschule mit Schwerpunkt Datenschutzrecht;
- Kenntnisse im Bereich der Informationssicherheit: mindestens zweijährige praktische Tätigkeit im Bereich der Informationssicherheit oder erfolgreich abgeschlossene, mindestens einjährige Ausbildung an einer Hochschule oder Fachhochschule mit Schwerpunkt Informationssicherheit;
- Kenntnisse der Entwicklungen im Bereich des Datenschutzrechts und im Bereich der Informationssicherheit;
- Fachkenntnisse bezüglich der Zertifizierung von Produkten, Dienstleistungen oder Prozessen, welche die Anforderungen des Zertifizierungsprogramms und der Richtlinien des EDÖB sowie die international massgebenden Anforderungen, insbesondere nach den technisch anwendbaren Normen und der Norm «SN EN ISO/IEC 17065[7], Konformitätsbewertung, Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren», erfüllen.

Die Zertifizierungsstelle muss für die einzelnen Bereiche über qualifiziertes Personal verfügen. Die Prüfung von Produkten, Dienstleistungen und Prozessen durch ein interdisziplinäres Team ist zulässig.

7 Die aufgeführte Norm kann kostenlos eingesehen und gegen Bezahlung bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.