Verordnung über die Datenschutzzertifizierungen (VDSZ)

vom 28. September 2007 (Stand am 1. Januar 2008)

Der Schweizerische Bundesrat,

gestützt auf Artikel 11 Absatz 2 des Bundesgesetzes vom 19. Juni 1992[1] über den Datenschutz (DSG),

verordnet:

1. Abschnitt: Zertifizierungsstellen

Art. 1 Anforderungen

1 Die Stellen, die Datenschutzzertifizierungen nach Artikel 11 DSG durchführen (Zertifizierungsstellen), müssen akkreditiert sein. Die Akkreditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[2], soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

2 Je eine separate Akkreditierung ist erforderlich für die Zertifizierung von:

a. Organisation und Verfahren des Datenschutzes;

b. Produkten (Hardware, Software oder Systeme für automatisierte Datenbearbeitungsverfahren).

3 Die Zertifizierungsstellen müssen über eine festgelegte Organisation sowie ein festgelegtes Zertifizierungsverfahren (Kontrollprogramm) verfügen. Darin müssen insbesondere geregelt sein:

a. die Begutachtungs- oder Prüfkriterien und die sich daraus ergebenden Anforderungen, welche die zu zertifizierenden Stellen oder Produkte zu erfüllen haben (Begutachtungs- bzw. Prüfungsraster); und

b. der Ablauf des Verfahrens, insbesondere das Vorgehen bei festgestellten Unregelmässigkeiten.

4 Die Mindestanforderungen an das Kontrollprogramm richten sich nach den gemäss Anhang 2 der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996 anwendbaren Normen und Grundsätzen sowie nach den Artikeln 4–6.

5 Die Mindestanforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt, richten sich nach dem Anhang.

AS **2007** 5003

1 SR **235.1**

2 SR **946.512**

Art. 2 Akkreditierungsverfahren

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

Art. 3 Ausländische Zertifizierungsstellen

[1] Der oder die Beauftragte anerkennt nach Rücksprache mit der Schweizerischen Akkreditierungsstelle ausländische Zertifizierungsstellen zur Tätigkeit auf schweizerischem Territorium, wenn diese eine gleichwertige Qualifikation wie die in der Schweiz geforderte nachweisen können.

[2] Die Zertifizierungsstellen haben insbesondere den Nachweis zu erbringen, dass sie die Anforderungen nach Artikel 1 Absätze 3 und 4 erfüllen und dass ihnen die schweizerische Datenschutzgesetzgebung hinreichend bekannt ist.

[3] Der oder die Beauftragte kann die Anerkennung befristen und mit Bedingungen oder Auflagen verbinden. Er oder sie entzieht die Anerkennung, wenn wesentliche Bedingungen und Auflagen nicht erfüllt werden.

2. Abschnitt: Gegenstand und Verfahren

Art. 4 Zertifizierung von Organisation und Verfahren

[1] Zertifizierbar sind:

a. die Gesamtheit der Datenbearbeitungsverfahren, für die eine Stelle verantwortlich ist;

b. einzelne, abgrenzbare Datenbearbeitungsverfahren.

[2] Gegenstand der Begutachtung ist das Datenschutzmanagementsystem. Dieses umfasst namentlich:

a. die Datenschutzpolitik;

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

c. die organisatorischen und technischen Vorkehrungen zur Verwirklichung der festgelegten Ziele und Massnahmen, insbesondere die Vorkehrungen zur Behebung festgestellter Mängel.

[3] Der oder die Beauftragte erlässt Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem. Er oder sie berücksichtigt dabei internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere die Normen ISO 9001:2000 und ISO 27001: 2005.

4 Die Ausnahme von der Pflicht zur Anmeldung von Datensammlungen nach Artikel 11*a* Absatz 5 Buchstabe f DSG ist nur anwendbar, wenn sämtliche Datenbearbeitungsverfahren, denen eine Datensammlung dient, zertifiziert sind.

Art. 5 Zertifizierung von Produkten

1 Zertifizierbar sind Produkte, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten, namentlich Daten über die Benutzerin oder den Benutzer, generiert werden.

2 Gegenstand der Prüfung ist namentlich die produktimmanente Gewährleistung:

a. von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der bearbeiteten Personendaten im Hinblick auf den Verwendungszweck des Produkts;

b. der Vermeidung der im Hinblick auf den Verwendungszweck des Produkts nicht erforderlichen Generierung, Speicherung oder anderen Bearbeitung von Personendaten;

c. von Transparenz und Nachvollziehbarkeit der automatisierten Bearbeitung von Personendaten, die im Rahmen der vom Hersteller festgelegten Funktionalität eines Produkts erfolgt;

d. von technischen Massnahmen zur Unterstützung des Anwenders oder der Anwenderin bei der Einhaltung weiterer Datenschutzgrundsätze und datenschutzrechtlicher Pflichten.

3 Der oder die Beauftragte erlässt bis spätestens am 1. Januar 2010 Richtlinien darüber, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind.

Art. 6 Erteilung und Gültigkeit der Datenschutzzertifizierung

1 Die Zertifizierung wird erteilt, wenn das Zertifizierungsverfahren aufgrund der von der Zertifizierungsstelle angewandten Begutachtungs- oder Prüfkriterien zum Ergebnis führt, dass die datenschutzrechtlichen Anforderungen sowie die Anforderungen, die sich aus dieser Verordnung und den von dem oder der Beauftragten erlassenen Richtlinien (Art. 4 Abs. 3 und 5 Abs. 3) oder anderen gleichwertigen Normen und Standards ergeben, erfüllt werden. Die Zertifizierung kann mit Bedingungen oder Auflagen verbunden werden.

2 Die Zertifizierung eines Datenschutzmanagementsystems ist während drei Jahren gültig. Die Zertifizierungsstelle hat jährlich summarisch zu überprüfen, ob die Voraussetzungen für die Zertifizierung weiterhin erfüllt sind.

3 Die Zertifizierung eines Produktes ist während zwei Jahren gültig. Ein Produkt muss erneut zertifiziert werden, sobald daran wesentliche Veränderungen vorgenommen wurden.

Art. 7 Anerkennung ausländischer Datenschutzzertifizierungen

Der oder die Beauftragte anerkennt nach Rücksprache mit der Schweizerischen Akkreditierungsstelle ausländische Zertifizierungen, wenn Gewähr dafür besteht, dass die Anforderungen der schweizerischen Gesetzgebung erfüllt werden.

Art. 8 Mitteilung des Ergebnisses des Zertifizierungsverfahrens

1 Teilt die Stelle, die eine Zertifizierung erhalten hat, dem oder der Beauftragten die erfolgreich absolvierte Zertifizierung nach Artikel 4 mit, um nach Artikel 11*a* Absatz 5 Buchstabe f DSG von der Pflicht zur Anmeldung ihrer Datensammlungen befreit zu werden, so hat sie auf Anfrage folgende Unterlagen einzureichen:

a. Bewertungsbericht;

b. Zertifizierungsdokumente.

2 Stellt die Zertifizierungsstelle im Rahmen ihrer Überwachungstätigkeit wesentliche Änderungen der Zertifizierungsvoraussetzungen fest, beispielsweise betreffend die Erfüllung von Bedingungen oder Auflagen, so ist der oder die Beauftragte von der Stelle, die die Zertifizierung erhalten hat, darüber zu informieren.

3 Der oder die Beauftragte veröffentlicht ein Verzeichnis der Stellen, die eine Zertifizierung erhalten haben und von der Pflicht zur Registrierung ihrer Datensammlungen befreit sind (Art. 28 Abs. 3 der V vom 14. Juni 1993[3] zum Datenschutzgesetz). Dieses Verzeichnis gibt namentlich über die Gültigkeitsdauer der Zertifizierung Auskunft.

3. Abschnitt: Sanktionen

Art. 9 Sistierung und Entzug der Zertifizierung

1 Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, namentlich wenn sie im Rahmen der Überprüfung (Art. 6 Abs. 2) schwere Mängel feststellt. Ein schwerer Mangel liegt insbesondere vor, wenn:

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

b. eine Zertifizierung in irreführender oder missbräuchlicher Art und Weise 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 Vertragsverhältnis zwischen Zertifizierungsstelle und Stelle, die die Zertifizierung erhalten hat, anwendbar sind.

3 Die Zertifizierungsstelle informiert den Beauftragten oder die Beauftragte über die Sistierung oder den Entzug der Datenschutzzertifizierung, wenn ihm oder ihr die Zertifizierung nach Artikel 8 Absatz 1 mitgeteilt wurde.

3 SR **235.11**

Art. 10 Verfahren bei Aufsichtsmassnahmen des oder der Beauftragten

[1] Stellt der oder die Beauftragte bei der Aufsichtstätigkeit nach Artikel 27 oder 29 DSG bei einer Stelle, die eine Zertifizierung erhalten hat, schwere Mängel fest, so unterrichtet er oder sie die Zertifizierungsstelle darüber.

[2] Die Zertifizierungsstelle veranlasst unverzüglich, dass die Stelle, die die Zertifizierung erhalten hat, den Mangel innert 30 Tagen ab dem Eingang der Mitteilung des oder der Beauftragten behebt.

[3] Behebt die Stelle, die die Zertifizierung erhalten hat, den Mangel nicht innerhalb dieser Frist, so sistiert die Zertifizierungsstelle die Zertifizierung. Besteht keine Aussicht darauf, dass innert einem angemessenen Zeitraum ein rechtskonformer Zustand geschaffen oder wiederhergestellt wird, so ist die Zertifizierung zu entziehen.

[4] Hat innert der Frist nach Absatz 2 die Stelle, die die Zertifizierung erhalten hat, den Mangel nicht behoben und die Zertifizierungsstelle die Zertifizierung nicht sistiert oder entzogen, so richtet der oder die Beauftragte eine Empfehlung nach Artikel 27 Absatz 4 oder Artikel 29 Absatz 3 DSG an die Stelle, die die Zertifizierung erhalten hat, oder an die Zertifizierungsstelle. Er kann der Zertifizierungsstelle namentlich empfehlen, die Zertifizierung zu sistieren oder zu entziehen. Richtet er die Empfehlung an die Zertifizierungsstelle, so informiert er die Schweizerische Akkreditierungsstelle darüber.

4. Abschnitt: Inkrafttreten

Art. 11

Diese Verordnung tritt am 1. Januar 2008 in Kraft.

Anhang
(Art. 1 Abs. 5)

Mindestanforderungen an die Qualifikation des Personals der Zertifizierungsstellen, welches Zertifizierungen durchführt

1 Zertifizierung von Datenschutzmanagementsystemen

Die Zertifizierungsstelle muss nachweisen, dass das Personal, welches Datenschutzmanagementsysteme zertifiziert, gesamthaft folgende Qualifikationen hat:

- Kenntnisse des Datenschutzrechts: Nachzuweisen ist eine mindestens zweijährige praktische Tätigkeit im Bereich des Datenschutzes oder eine erfolgreich abgeschlossene Ausbildung an einer Hochschule oder Fachhochschule von mindestens einem Jahr Dauer mit Schwerpunkt Datenschutzrecht;
- Kenntnisse im Bereich der Informatiksicherheit: Nachzuweisen ist eine mindestens zweijährige praktische Tätigkeit im Bereich der Informatiksicherheit oder eine erfolgreich abgeschlossene Ausbildung an einer Hochschule oder Fachhochschule von mindestens einem Jahr Dauer mit Schwerpunkt Informatiksicherheit;
- Ausbildung als Auditorin oder Auditor von Managementsystemen (nach ISO/IEC-Guide 62 [ISO/IEC 17021:2006]).

Die Zertifizierungsstelle muss nachweisen, dass sie jeweils für die einzelnen Teilbereiche über qualifiziertes Personal verfügt. Die Begutachtung der Datenschutzmanagementsysteme durch ein interdisziplinäres Team ist zulässig.

2 Zertifizierung von Produkten

Die Zertifizierungsstelle muss nachweisen, dass das Personal, welches Produkte zertifiziert, gesamthaft folgende Qualifikationen hat:

- Kenntnisse des Datenschutzrechts: Nachzuweisen ist eine mindestens zweijährige praktische Tätigkeit im Bereich des Datenschutzes oder eine erfolgreich abgeschlossene Ausbildung an einer Hochschule oder Fachhochschule von mindestens einem Jahr Dauer mit Schwerpunkt Datenschutzrecht;
- Kenntnisse im Bereich der Informatiksicherheit: Nachzuweisen ist eine mindestens zweijährige praktische Tätigkeit im Bereich der Informatiksicherheit oder eine erfolgreich abgeschlossene Ausbildung an einer Hochschule oder Fachhochschule von mindestens einem Jahr Dauer mit Schwerpunkt Informatiksicherheit;
- Fachkenntnisse bezüglich der Produkteprüfung (nach ISO/IEC-Guide 65).

Die Zertifizierungsstelle muss nachweisen, dass sie jeweils für die einzelnen Teilbereiche über qualifiziertes Personal verfügt. Die Produkteprüfung durch ein interdisziplinäres Team ist zulässig.