Verordnung über die Datenschutzzertifizierungen (VDSZ)

Entwurf vom
1. Februar 2007

vom ...

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] Stellen, die Datenschutzzertifizierungen nach Artikel 11 DSG durchführen (Zertifizierungsstellen), müssen für ihre Tätigkeit akkreditiert sein. Die Akkreditierung der Zertifizierungsstellen 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 (Programme und Systeme).

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

a. 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 ein geeignetes Konzept für 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 **1993** 1962
[1] SR **235.1**
[2] SR **946.512**

Art. 2 Akkreditierungsverfahren

Die Schweizerische Akkreditierungsstelle zieht für das Akkreditierungsverfahren und die Nachkontrolle 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 die Anforderungen nach Artikel 1 Absätze 3 und 4 erfüllt werden und dass die schweizerische Datenschutzgesetzgebung hinreichend bekannt ist.

[3] Der oder die Beauftragte kann die Anerkennung befristen und mit Bedingungen oder Auflagen verbinden. Er oder sie hebt die Anerkennung auf, 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] Die Mindestanforderungen an das Datenschutzmanagementsystem richten sich nach den internationalen Normen für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere bezüglich der Datensicherheit (Norm 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 Softwareprodukte oder Kombinationen von Softwareprodukten mit bestimmten Hardwareprodukten, 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 sind namentlich die produkt- bzw. systemimmanente Gewährleistung der:

a. im Hinblick auf den Verwendungsweck des Produkts oder Systems erforderlichen technischen Massnahmen zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der bearbeiteten Personendaten;

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

c. Transparenz und Nachvollziehbarkeit der im Rahmen der Erfüllung der vom Hersteller festgelegten Funktionalität eines Produkts automatisiert erfolgenden Bearbeitung von Personendaten.

3 Der oder die Beauftragte erlässt 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 weitere Anforderungen, die sich aus den Anhängen 1 und 2 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 Veränderungen vorgenommen wurden.

Art. 7 Anerkennung ausländischer Datenschutzzertifizierungen

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

Art. 8 Mitteilung des Ergebnisses des Zertifizierungsverfahrens

1 Teilt die zertifizierte Stelle die erfolgreich absolvierte Zertifizierung nach Artikel 4 der oder dem Beauftragten 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 die oder der Beauftragte von der zertifizierten Stelle darüber zu informieren.

3 Die oder der Beauftragte veröffentlicht eine Liste der zertifizierten Stellen, die von der Pflicht zur Registrierung ihrer Datensammlungen befreit sind. Die Liste gibt namentlich über die Gültigkeitsdauer der Zertifizierung Auskunft.

3. Abschnitt: Sanktionen

Art. 9 Sistierung und Entzug der Zertifizierung

1 Die Zertifizierungsstelle kann eine bestehende Zertifizierung sistieren oder entziehen, namentlich wenn im Rahmen der Überprüfung (Art. 6 Abs. 2) schwere Mängel festgestellt werden. 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 auf das Vertragsverhältnis zwischen Zertifizierungsstelle und zertifizierter Stelle anwendbaren zivilrechtlichen Bestimmungen.

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

Art. 10 Verfahren bei Aufsichtsmassnahmen der oder des Beauftragten

1 Stellt die oder der Beauftragte bei seiner Aufsichtstätigkeit nach Artikel 27 oder 29 DSG bei einer zertifizierten Stelle schwere Mängel fest, so unterrichtet sie oder er die Zertifizierungsstelle darüber.

2 Die Zertifizierungsstelle veranlasst unverzüglich, dass die für die Erfüllung der Zertifizierungsvoraussetzungen oder die Gewährleistung einer rechtmässigen Ver-

wendung der Zertifizierung erforderlichen Massnahmen innert 30 Tagen ab dem Eingang der Mitteilung des oder der Beauftragten getroffen werden.

3 Behebt die zertifizierte Stelle 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 weder die zertifizierte Stelle den Mangel behoben noch die Zertifizierungsstelle die Zertifizierung sistiert oder entzogen, so richtet die oder der Beauftragte eine Empfehlung nach Artikel 27 Absatz 4 oder Artikel 29 Absatz 3 DSG an die zertifizierte Stelle 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: Schlussbestimmung

Art. 11 Inkrafttreten

Diese Verordnung tritt am ...2007 in Kraft.

Anhang

(Art. 1 Abs. 5)

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

1 Zertifizierung von Datenschutzmanagementsystemen

Die Zertifizierungsstelle muss bezüglich ihres Personals, welches Zertifizierungen von Datenschutzmanagementsystemen durchführt, folgende Qualifikationen nachweisen:

- 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 mind. 1 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 mind. 1 Jahr Dauer mit Schwerpunkt Informatiksicherheit.
- Ausbildung als Auditorin/Auditor von Managementsystemen (nach ISO/IEC-Guide 62 [ISO/IEC 17021:...]).

Die Zertifizierungsstelle kann nachweisen, dass sie jeweils für die einzelnen Teilbereiche über qualifiziertes Personal verfügt. Die Durchführung des Audits durch ein interdisziplinäres Team ist zulässig.

2 Zertifizierung von Produkten

Die Zertifizierungsstelle muss bezüglich ihres Personals, welches Produktezertifizierungen durchführt, folgende Qualifikationen nachweisen:

- 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 mind. 1 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 mind. 1 Jahr Dauer mit Schwerpunkt Informatiksicherheit;

- Fachkenntnisse bezüglich der Produkteprüfung (nach ISO/IEC-Guide 65).

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