Liechtensteinisches Landesgesetzblatt
Jahrgang 2013 Nr. 403 ausgegeben am 13. Dezember 2013

Verordnung
vom 10. Dezember 2013
über die Datenschutzzertifizierungen (VDSZ)

Aufgrund von Art. 14a Abs. 2, Art. 15 Abs. 6 und Art. 42 Abs. 1 des Datenschutzgesetzes (DSG) vom 14. März 2002, LGBl. 2002 Nr. 55, in der geltenden Fassung, verordnet die Regierung:

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Bezeichnungen

1) Diese Verordnung regelt zur Verbesserung des Datenschutzes und der Datensicherheit:

a) die Bewertung von Produkten, Systemen, Verfahren und Organisationen durch anerkannte unabhängige Zertifizierungsstellen; und

b) das Datenschutz-Qualitätszeichen.

2) Unter den in dieser Verordnung verwendeten Personen- und Funktionsbezeichnungen sind Angehörige des weiblichen und männlichen Geschlechts zu verstehen.

II. Zertifizierungsstellen

Art. 2

Anforderungen

1) Die Stellen, die Datenschutzzertifizierungen nach Art. 14a DSG durchführen (Zertifizierungsstellen), müssen auf der Grundlage der Norm ISO/IEC 17065 und den hier festgelegten Anforderungen akkreditiert sein. Die Akkreditierung richtet sich nach dem Gesetz über die Akkreditierung und Notifizierung, soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

2) Die Akkreditierung von Zertifizierungsstellen ist zulässig für die Zertifizierung von Produkten, Systemen, Verfahren und Organisationen im Sinne von Art. 5 Abs. 1. Die Akkreditierung kann auch getrennt für einzelne, in sich abgeschlossene Produkte, Systeme, Verfahren und Organisationen erfolgen.

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 6 der Verordnung über die Akkreditierung und Notifizierung anwendbaren Normen und Grundsätzen sowie nach Art. 5 bis 7.

5) Die Mindestanforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt, richten sich nach Anhang 1.

Art. 3

Akkreditierungsverfahren

Die Liechtensteinische Akkreditierungsstelle zieht für das Akkreditierungsverfahren und die Nachkontrolle sowie für die Sistierung oder den Entzug einer Akkreditierung die Datenschutzstelle nach Art. 32 Abs. 1 Bst. h DSG bei.

Art. 4

Ausländische Zertifizierungsstellen

1) Die Liechtensteinische Akkreditierungsstelle anerkennt nach Rücksprache mit der Datenschutzstelle ausländische Zertifizierungsstellen zur Tätigkeit auf dem liechtensteinischen Territorium, wenn diese eine gleichwertige Qualifikation wie die in Liechtenstein geforderte nachweisen können.

2) Die Zertifizierungsstellen haben insbesondere den Nachweis zu erbringen, dass sie die Anforderungen nach Art. 2 Abs. 3 und 4 erfüllen und ihnen die liechtensteinische Datenschutzgesetzgebung hinreichend bekannt ist.

3) Die Liechtensteinische Akkreditierungsstelle kann die Anerkennung befristen und mit Bedingungen oder Auflagen verbinden. Sie entzieht die Anerkennung, wenn wesentliche Bedingungen und Auflagen nicht erfüllt werden.

III. Gegenstand und Verfahren

Art. 5

Gegenstand von Zertifizierungen

1) Gegenstand eines Zertifizierungsverfahrens nach Art. 6 können Produkte, Systeme, Verfahren und Organisationen sein. Hierzu zählen insbesondere (informationstechnische) Produkte wie Hardware, Software, Systeme, automatisierte Organisationen und Verfahren (Datenschutzmanagementsysteme) sowie Dienstleistungen.

2) Zertifizierbar sind:

a) die Gesamtheit aller Produkte, Systeme, Verfahren und Organisationen, für die eine Stelle verantwortlich ist;

b) einzelne, abgrenzbare Produkte, Systeme, Verfahren und Organisationen.

3) Zertifizierbar sind ausschliesslich Produkte, Systeme, Verfahren und Organisationen, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten, namentlich Daten über den Benutzer, generiert werden.

4) Die Zertifizierung von Produkten, Systemen, Verfahren und Organisationen umfasst namentlich:

a) die Dokumentation von Zielen und Massnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit (Datenschutzpolitik und -konzept);

b) die organisatorischen und technischen Vorkehrungen zur Verwirklichung der festgelegten Ziele und Massnahmen, insbesondere die Vorkehrungen zur Behebung festgestellter Mängel sowie zur Revisionsfähigkeit der Datenbearbeitung.

5) Gegenstand der Prüfung ist insbesondere die dem Zertifizierungsgegenstand immanente Gewährleistung:

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

b) der Vermeidung der im Hinblick auf den Verwendungszweck des Zertifizierungsgegenstandes 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, Systems, Verfahrens oder einer Organisation erfolgt;

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

6) Die Datenschutzstelle erlässt einen Katalog datenschutzspezifischer Kriterien, die im Rahmen der Zertifizierung mindestens zu prüfen sind. Neben der liechtensteinischen Gesetzgebung sind dabei internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere die Normen ISO 9001 und ISO 27001 sowie die Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie, insbesondere die Normen ISO/IEC 15408, 17065 und Common Criteria, zu berücksichtigen. Die Datenschutzstelle veröffentlicht den Katalog der datenschutzspezifischen Kriterien in geeigneter Art und Weise, insbesondere über ihre Internetseite.

Art. 6

Zertifizierungsverfahren

1) Die für die Zertifizierung verantwortliche Stelle hat den Antrag auf Zertifizierung von Produkten, Systemen, Verfahren und Organisationen nach Art. 14a DSG schriftlich bei einer nach Art. 2 akkreditierten Zertifizierungsstelle einzureichen.

2) Die Datenschutzstelle ist zum Zweck der Prüfung nach Art. 32 Abs. 1 Bst. h DSG zu dem Zertifizierungsverfahren beizuziehen. Die Zertifizierungsstelle hat der Datenschutzstelle den Antrag unverzüglich zur Prüfung vorzulegen. Auf Anfrage der Datenschutzstelle sind dieser jederzeit alle weiteren für das Zertifizierungsverfahren erforderlichen Informationen bekannt zu geben.

3) Nach Abschluss der Prüfung durch die Zertifizierungsstelle hat diese die Datenschutzstelle über das Ergebnis der Prüfung zu informieren. Die Information hat zu enthalten:

a) die Bezeichnung der verantwortlichen Stelle und des zertifizierten Gegenstandes;

b) den Bewertungsbericht.

4) Die Zertifizierungsstelle darf die Zertifizierung erst nach Mitteilung der Datenschutzstelle über eine erfolgreich absolvierte Prüfung nach Art. 32 Abs. 1 Bst. h DSG erteilen.

5) Die Datenschutzstelle verrechnet ihren Prüfungsaufwand nach Art. 32 Abs. 1 Bst. h DSG mit einem Stundensatz von 130 Franken. Von diesem Stundensatz kann abgewichen werden, wenn dies aufgrund besonderer Umstände notwendig ist. Liegen besondere Umstände vor, so informiert die Datenschutzstelle die Zertifizierungsstelle im Voraus über den zur Anwendung kommenden Stundensatz.

Art. 7

Erteilung und Gültigkeit der Datenschutzzertifizierung

1) Die Zertifizierung wird erteilt, wenn das Zertifizierungsverfahren aufgrund der von der Zertifizierungsstelle angewandten Begutachtungs- oder Prüfkriterien und der Prüfung der Datenschutzstelle zum Ergebnis führt, dass die datenschutzrechtlichen Anforderungen sowie die Anforderungen, die sich aus dieser Verordnung und dem nach Art. 5 Abs. 6 von der Datenschutzstelle veröffentlichten Kriterienkatalog oder anderen gleichwertigen

Normen und Standards ergeben, erfüllt werden. Die Zertifizierung kann mit Bedingungen oder Auflagen verbunden werden.

2) Eine erteilte Zertifizierung ist während drei Jahren gültig. Die Zertifizierungsstelle hat jährlich zu überprüfen, ob die Voraussetzungen für die Zertifizierung weiterhin erfüllt sind.

3) Stellt die Zertifizierungsstelle im Rahmen ihrer Überwachungstätigkeit wesentliche Änderungen der Zertifizierungsvoraussetzungen fest, beispielsweise betreffend die Erfüllung von Bedingungen oder Auflagen, so hat sie die Datenschutzstelle darüber unverzüglich zu informieren.

4) Zertifizierte Produkte, Systeme, Verfahren und Organisationen können durch ein Datenschutz-Qualitätszeichen nach Anhang 2 gekennzeichnet werden. Das Datenschutz-Qualitätszeichen muss das graphische Symbol, die Verzeichnisnummer, das Datum des Ablaufs der Gültigkeit nach Abs. 2 und die Adresse der Internetseite der Datenschutzstelle enthalten. Die Farben sind Schwarz, Blau, Rot und Gold. Eine Darstellung in entsprechenden Grautönen ist möglich. Das Datenschutz-Qualitätszeichen kann unter Wahrung der Proportionen seiner Bestandteile in jeder beliebigen Gesamtgrösse verwendet werden.

Art. 8

Mitteilung des Ergebnisses des Zertifizierungsverfahrens

1) Zertifizierungsstellen haben die Datenschutzstelle unverzüglich über eine erteilte Zertifizierung zu informieren.

2) Die verantwortliche Stelle ist nach Art. 15 Abs. 6 DSG von der Pflicht zur Anmeldung zum Register der Datensammlungen befreit. Die Befreiung gilt nur, wenn sämtliche Produkte, Systeme, Verfahren und Organisationen zertifiziert sind, welche einer Datensammlung dienen.

3) Die Datenschutzstelle veröffentlicht auf ihrer Internetseite mittels Abrufverfahren ein Verzeichnis der verantwortlichen Stellen. Das Verzeichnis hat die Bezeichnung der verantwortlichen Stelle und des zertifizierten Gegenstandes aufzuführen sowie Auskunft darüber zu erteilen, ob die verantwortliche Stelle nach Abs. 2 von der Pflicht zur Anmeldung ihrer Datensammlungen befreit ist.

Art. 9

Anerkennung ausländischer Datenschutzzertifizierungen

Die Liechtensteinische Akkreditierungsstelle anerkennt nach Rücksprache mit der Datenschutzstelle ausländische Zertifizierungen, wenn die hierfür verantwortliche Stelle den Nachweis erbracht hat, dass die Anforderungen nach Art. 5 erfüllt werden.

IV. Sanktionen

Art. 10

Sistierung und Entzug der Zertifizierung

1) Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, insbesondere wenn sie im Rahmen der Überprüfung (Art. 7 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 verantwortlicher Stelle anwendbar sind.

3) Die Zertifizierungsstelle informiert die Datenschutzstelle unverzüglich über die Sistierung oder den Entzug der Datenschutzzertifizierung.

Art. 11

Verfahren bei Aufsichtsmassnahmen der Datenschutzstelle

1) Stellt die Datenschutzstelle bei der Aufsichtstätigkeit nach Art. 29 oder 30 DSG bei einer verantwortlichen Stelle schwere Mängel fest, so unterrichtet sie die Zertifizierungsstelle unverzüglich darüber.

2) Die Zertifizierungsstelle veranlasst unverzüglich, dass die verantwortliche Stelle den Mangel innert 30 Tagen ab dem Eingang der Mitteilung der Datenschutzstelle behebt.

3) Behebt die verantwortliche 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 Abs. 2 die verantwortliche Stelle den Mangel nicht behoben und die Zertifizierungsstelle die Zertifizierung nicht sistiert oder entzogen, so richtet die Datenschutzstelle eine Empfehlung nach Art. 29 Abs. 4 oder Art. 30 Abs. 3 DSG an die verantwortliche Stelle oder an die Zertifizierungsstelle. Sie kann der Zertifizierungsstelle namentlich empfehlen, die Zertifizierung zu sistieren oder zu entziehen. Richtet die Datenschutzstelle die Empfehlung an die Zertifizierungsstelle, so informiert sie die Liechtensteinische Akkreditierungsstelle darüber.

V. Schweigepflicht

Art. 12

Grundsatz

Von den Behörden zum Verfahren beigezogene Dritte, insbesondere Gutachter und Sachverständige, haben über die ihnen im Rahmen ihrer Tätigkeit zur Kenntnis gelangten Geschäfts- oder Betriebsgeheimnisse Stillschweigen zu bewahren. Sie unterstehen im Rahmen ihrer Tätigkeit dem Amtsgeheimnis.

VI. Schlussbestimmung

Art. 13

Inkrafttreten

Diese Verordnung tritt am 1. Februar 2014 in Kraft.

Fürstliche Regierung:
gez. *Adrian Hasler*
Fürstlicher Regierungschef

Anhang 1

(Art. 2 Abs. 5)

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

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

a) 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;

b) 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;

c) Ausbildung als Auditor von Managementsystemen (nach ISO/IEC 17021) bzw. Fachkenntnisse bezüglich der Produkteprüfung (nach ISO/IEC 17065).

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

Anhang 2

(Art. 7 Abs. 4)

Datenschutz-Qualitätszeichen