Information Security Society Switzerland

IT & LAW CONSULTING GMBH

Stellenwert und praktische Bedeutung der Zertifizierung von Datenschutz-Managementsystemen nach DSGVO und DSG

27. Juni 2017

ISSS Zürcher Tagung 2017

mag. iur. Maria Winkler
IT & Law Consulting GmbH

Inhaltsverzeichnis

- Ausgangslage (CH und EU)
  - Selbstregulierung
  - Gegenstand der Zertifizierung
  - Rechtswirkungen
  - Gültigkeit und Entzug
- Praxis
  - Aufbau eines DSMS nach VDSZ
  - Elemente eines DSMS
  - Compliance
  - Stolpersteine
- Schlussfolgerungen

Ausgangslage (CH und EU)

Selbstregulierung

- Das geltende Datenschutzgesetz (Art. 11 DSG) sowie der Vorentwurf des revidierten DSG (Art. 10 VE-DSG) sehen eine **fakultative Zertifizierung** vor.
- Die ausführenden Bestimmungen sind in der **Verordnung über die Datenschutzzertifizierungen (VDSZ)** und den begleitenden Dokumenten enthalten.
- Für Krankenversicherer ist die Zertifizierung ihrer Datenannahmestellen in der Schweiz **verpflichtend** (Art. 59a KVV).
- Die EU-Datenschutzgrundverordnung (DSGVO) weist die Mitgliedsstaaten, die Aufsichtsbehörden, den Ausschuss und die Kommission an, Zertifizierungsverfahren zu fördern. Die Zertifizierungen **müssen freiwillig** sein (Art. 42 Abs. 3 DSGVO).

Ausgangslage (CH)

Gegenstand der Zertifizierung (Geltendes Recht)

- Zertifizierbar sind:
  - die **Gesamtheit der Datenbearbeitungsverfahren**, für die eine Stelle verantwortlich ist;
  - einzelne, **abgrenzbare Datenbearbeitungsverfahren.**
- **Dienstleistungen** können nach VDSZ nicht zertifiziert werden.
- **Produkte** (Hardware, Software oder Systeme für automatisierte Datenbearbeitungen) können gemäss Art. 5 VDSZ zertifiziert werden. Die dafür erforderlichen Richtlinien wurden aber durch den EDÖB noch nicht erlassen.

Ausgangslage (CH)

Gegenstand der Zertifizierung (VE-DSG)

- Der Vorentwurf des revidierten DSG (VE-DSG) sieht vor, dass Verantwortliche und Auftragsbearbeiter ihre **Datenbearbeitungsvorgänge** zertifizieren lassen können (Art. 10 VE-DSG).
- In Zukunft sollen daher neben Datenbearbeitungssystemen (Verfahren, Organisation) und Produkten (Programme, Systeme) auch **Dienstleistungen** zertifiziert werden können.

Ausgangslage (EU)

Gegenstand der Zertifizierung (DSGVO)

- Zertifiziert werden **Verarbeitungsvorgänge** von Verantwortlichen oder Auftragsverarbeitern, die unter die DSGVO fallen (Art. 42 Abs. 1 DSGVO).
- **Zertifizierungen,** die spezifisch auf die Rechtfertigung von **Datenexporten in Drittländer** ausgerichtet sind, können als Nachweis geeigneter Garantien für solche Datenexporte dienen (Art. 42 Abs. 2 DSGVO i.V.m Art. 46 Abs. 2 Bst. f DSGVO). Voraussetzung ist, dass sich der Datenempfänger im Drittland nicht nur zertifizieren lässt sondern auch zusätzlich (vertraglich) verpflichtet, diese Garantien einzuhalten.

Ausgangslage

- **Verordnung über die Datenschutzzertifizierungen (VDSZ)**
  - Zertifiziert wird ein **Datenschutzmanagementsystem**
  - Elemente des DSMS sind beispielsweise eine Politik, Weisungen, die Regelung von Verantwortlichkeiten, interne Audits
  - Ziel: Systematische Gewährleistung des Datenschutzes (Plan-Do –Act – Check)

- **Datenschutz-Grundverordnung (DSGVO)**
  - Zertifiziert wird die Einhaltung der DSGVO
  - Ziel: **Nachweis der Compliance**
  - Problem: Im Rahmen des Audits wird eine Momentaufnahme gemacht, das Zertifikat bestätigt die Compliance nur im Zeitpunkt der Zertifizierung
  - Zurzeit fehlen in vielen EU-Ländern noch die entsprechenden Ausführungsbestimmungen

Ausgangslage

Rechtswirkungen (CH)

- Die datenbearbeitende Stelle (Verantwortlicher oder Auftragsbearbeiter) bleibt trotz Zertifizierung für die Einhaltung des Datenschutzes verantwortlich.
- Die Meldung der Zertifizierung an den EDÖB befreit das Unternehmen im zertifizierten Bereich von der Meldepflicht für Datensammlungen (Art. 11a Abs. 5 lit. f DSG).
- Eine Zertifizierung kann beim **Nachweis des gesetzeskonformen Vorgehens** bzw. der **Einhaltung verschiedenster (zukünftiger) Prüf- und Dokumentationspflichten** helfen.
- **Beispiele**: Massnahmen der Datensicherheit (Art. 7 DSG; Art. 11 VE-DSG); Datenschutz-Folgeabschätzung (Art. 16 VE-DSG), Dokumentationspflicht (Art. 19 Abs. 1 VE-DSG); Privacy by Design (Art. 18 VE-DSG)
- Die Nichteinhaltung der Zertifizierungsvorgaben nach Erteilung des Zertifikats ist **nicht strafbar**.

Ausgangslage

Rechtswirkungen (DSGVO)

- Die Zertifizierung ändert nichts an der Verantwortung der datenbearbeitenden Stelle (Art. 42 Abs. 4 DSGVO).
- Die Zertifizierung kann aber als „Gesichtspunkt“ herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen (Art. 24 Abs. 3 DSGVO).
- Die Zertifizierung kann insbesondere **einen Datenexport in ein Drittland rechtfertigen**.
  - Die Zertifizierung muss ausdrücklich auf die **Rechtfertigung von Datenexporten** ausgelegt sein und
  - der Datenempfänger im Drittland muss sich rechtsverbindlich und durchsetzbar verpflichten, diese zertifizierten Garantien einzuhalten (z.B. durch einen Vertrag).
- Gibt das Unternehmen während der Zertifizierung nicht alle erforderlichen Informationen preis, ist dies strafbar (Art. 83 Abs. 4 lit. a DSGVO i.V.m. Art. 42 Abs. 6 DSGVO). Nicht strafbar (nach DSGVO) ist jedoch die Nichteinhaltung der Zertifizierungskriterien nach Erteilung der Zertifizierung.

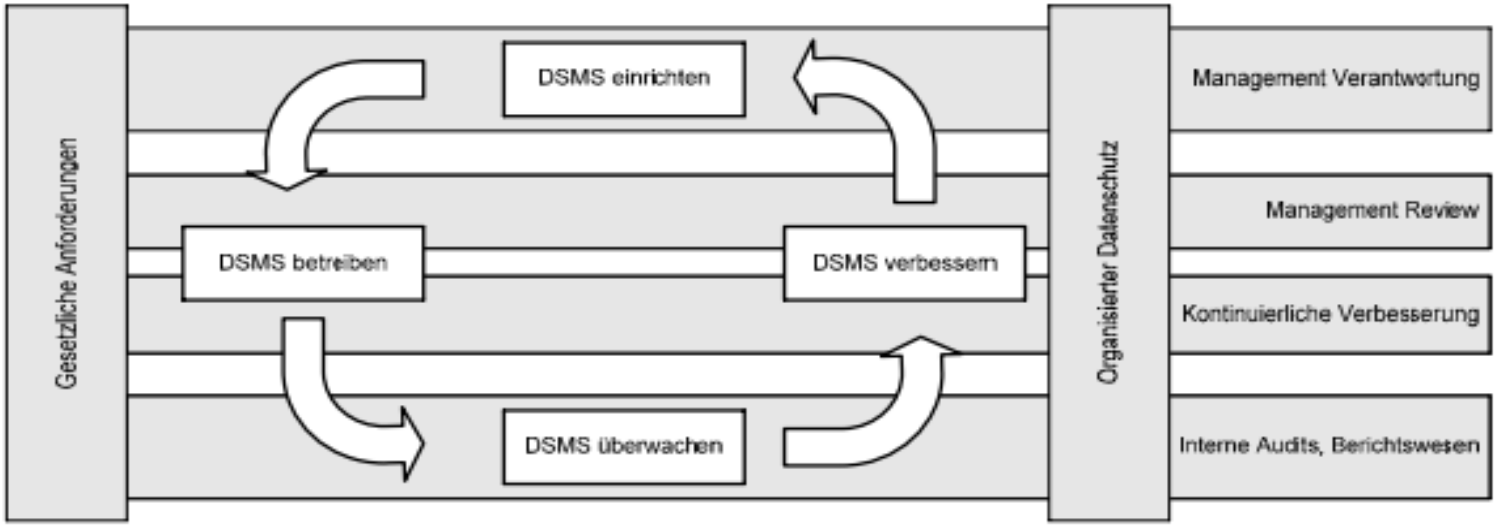
Ausgangslage

Gültigkeit und Entzug

- Zertifikate haben eine **Höchstdauer von 3 Jahren** (Art. 6 Abs. 2 VDSZ und Art. 42 Abs. 7 DSGVO). Während der dreijährigen Dauer finden Audits statt, mit denen geprüft wird, ob die Voraussetzungen noch erfüllt sind.
- Stellen die Zertifizierungsstelle oder der EDÖB bei einer Prüfung einen **schweren Mangel** fest, muss die Zertifizierungsstelle das Zertifikat **entziehen** (Art. 9 und 10 VDSZ)**.** Dies kann problematisch sein, wenn die Zertifizierungsstelle und der EDÖB sich in der Beurteilung des Mangels nicht einig sind .
- Die Zertifizierung kann durch die Zertifizierungsstelle oder durch die Aufsichtsbehörde **widerrufen** werden. Die Aufsichtsbehörde kann die Zertifizierungsstelle **anweisen**, das Zertifikat zu widerrufen (Art. 42 Abs. 7 DSGVO)**.**
- Bei einem Entzug bzw. Widerruf eines Zertifikats droht ein **Imageverlust**.

Praxis: Aufbau eines DSMS nach VDSZ

- Das DSMS basiert auf dem PDCA-Ansatz (Plan-Do-Check-Act).
- Ziel ist die **ständige Verbesserung des Datenschutzes** in der zertifizierten Organisation.



Quelle: Erläuterungen des BJ zur VDSZ, abrufbar unter https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/archiv/datenschutz/erl-vdsz-d.pdf

Praxis: Elemente eines DSMS

- Der Geltungsbereich des DSMS (Scope) muss klar beschrieben sein. Die Beschreibung umfasst:
  - die Datenbearbeitungsverfahren (alle oder nur einzelne);
  - die betroffenen Datensammlungen;
  - die relevanten technischen Systeme;
  - die betroffenen Standorte;
  - die Outsourcingpartner im zu zertifizierenden Bereich.
- Damit ein DSMS von einer externen Stelle auditiert und zertifiziert werden kann, muss eine **Dokumentation** erstellt werden. In der Praxis werden oft Software-Tools eingesetzt, welche das Management dieser Dokumente erleichtern.

Praxis: Compliance

- Regelung der Verantwortung
- Bestellung eines Datenschutzbeauftragten
- Erhebung der Datensammlungen
- Prüfung von Datenbearbeitungen
- Festlegung des Vorgehens bei Abweichungen
- Weisungen und Reglemente
- Schulung von Mitarbeitenden
- Etc.

- Fazit: Ein DSMS nach der VDSZ enthält zahlreiche Elemente, die mit der Revision des DSG voraussichtlich verpflichtend eingeführt werden!

Praxis: Stolpersteine

- Der Geltungsbereich des DSMS ist nicht klar definiert.
- Das Management steht nicht hinter dem Zertifizierungsentscheid.
- Die Organisation setzt sich nicht oder zu wenig mit den Anforderungen der VDSZ inklusive ISO/IEC 27001:2013 auseinander.
- Der Dokumentationsaufwand wird unterschätzt. Insbesondere die Anwendbarkeitserklärung (SoA = Statement of Applicability) wird nicht oder nur sehr spärlich erstellt.
- Nach dem Aufbau und der Erstzertifizierung muss der systematische Betrieb des DSMS oft erst „erlernt“ werden.

Schlussfolgerungen

- Der Erwerb eines Datenschutz-Zertifikats ändert nichts an der Verantwortung des Unternehmens.
- Eine Zertifizierung kann aber den Nachweis der Einhaltung von Sorgfaltspflichten, Dokumentationspflichten aber auch des gesetzeskonformen Vorgehens erleichtern.
- Zertifizierungen können in Zukunft auch die Zusammenarbeit mit Unternehmen in der EU erleichtern. Allerdings bleibt abzuwarten, ob eine Zertifizierung nach VDSZ auch in der EU anerkannt wird.
- Mit dem Aufbau eines DSMS nach der VDSZ erfüllen Unternehmen bereits zahlreiche Dokumentations- und Nachweispflichten, die mit der Revision des DSG voraussichtlich eingeführt werden.

Besten Dank für Ihre Aufmerksamkeit

Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug

Tel. +41 41 711 74 08
Fax +41 41 711 74 07
maria.winkler@itandlaw.ch
www.itandlaw.ch