VISCHER

IT-Security-Standards: Feigenblatt oder Musterlösung für Datenschutz-Compliance?

An: CLOUD 2019 Infrastruktur & Security Fachkongress

Von: Rolf Auf der Maur und Elias Mühlemann, VISCHER AG

Datum: 29. Oktober 2019

4421718.1

Betrifft: Handout zum Workshop

I. EINLEITUNG

Das folgende Handout gewährt einen kurzen Überblick über das Zusammenwirken von Datenschutz und Datensicherheit – zwei Themenkreise, die eng miteinander verzahnt sind. Wohl gerade deshalb werden diese Begriffe häufig unzureichend voneinander unterschieden. Einleitend deshalb eine Abgrenzung:

- "**Datensicherheit**" bezieht sich auf den Schutz **jeglicher Art von Daten** vor Manipulation, Verlust und unberechtigter Kenntnisnahme.
- "**Datenschutz**" schreibt vor, welche **personenbezogenen Daten** wie bearbeitet werden dürfen bzw. wie deren Verfügbarkeit, Vertraulichkeit und Integrität geschützt werden muss. Diese Vorgaben beziehen sich auch auf die Sicherheit von Personendaten.

Nachfolgend erfolgt zunächst ein kurzer Überblick der rechtlichen Anforderungen in der Schweiz zur Datensicherheit (Ziff. II) sowie zum Datenschutz (Ziff. III). Sodann gehen wir insbesondere darauf ein, inwiefern die im Bereich der Datensicherheit weit verbreiteten Standards auch zur Datenschutz-Compliance verhelfen können – oder gerade nicht. Dazu erfolgt eine Aufstellung zur Funktionsweise von Standards im Allgemeinen (Ziff. IV) sowie einer Einschätzung, inwiefern die Befolgung von (IT-Security-) Standards zur Datenschutz-Compliance beitragen können (Ziff. V).

II. GESETZLICHE ANFORDERUNGEN BZGL. DATENSICHERHEIT

In der Schweiz besteht kein umfassendes Gesetz betreffend Datensicherheit bzw. IT-Sicherheit. Allerdings ergeben sich Verpflichtungen zur Datensicherheit sowohl aus der allgemeinen Organisationsverantwortung von Organen (nachfolgend A.) als auch aus objekt- und sektorspezifischen Regulierungen (nachfolgend B.).

A. Datensicherheit ist Chefsache!

Den Organen von Handelsgesellschaften obliegt die unübertragbare und unentziehbare Verantwortung zur Organisation der Gesellschaft

(Art. 716a OR). Sie sind insbesondere dazu verpflichtet, das Risikomanagement der Gesellschaft und die operative Sicherheit zu gewährleisten. Je nach Unternehmensart bildet das Management von Cyber-Risiken ein wesentlicher Bestandteil dieser Verantwortung.

Ein **Cyber-Risikomanagement-Konzept** beinhaltet mindestens:

- Identifikation der Cyber-Bedrohungspotentiale, insbesondere für kritische/sensitive Daten und Systeme.
- Schutz der Geschäftsprozesse und IT-Infrastruktur.
- Reaktionsplan im Falle eines Cyber-Angriffs.

Kommen die Organe dieser Verpflichtung nicht nach, so können sie sich persönlich haftbar machen: Der Verwaltungsrat und weitere mit der Geschäftsführung beauftragte Personen haften gegenüber der Gesellschaft, den Aktionären und Gläubigern für pflichtwidrig und schuldhaft verursachte Schäden (Organisationsverschulden).

- ➢ Der VR ist verpflichtet, sich das notwendige Wissen betreffend IT-Sicherheit der Gesellschaft anzueignen (meist durch Dritte) und entsprechend fundierte Massnahmen zu treffen.
- ➢ Die Vernachlässigung von Cyber-Risiken kann **zur persönlichen Haftung** von Verwaltungsräten und Geschäftsleitungsmitgliedern führen.

B. Objekt- und branchenspezifische Anforderungen

Auch wenn in der Schweiz kein "Datensicherheitsgesetz" existiert, so sind doch in ausgewählten Bereichen spezifische gesetzliche Verpflichtungen betreffend Datensicherheit festgehalten. Diese ergeben sich einerseits aus *direkten* Verpflichtungen zur Sicherung von Infrastruktur (Systeme, Produkte, Daten) oder *indirekt* aus Geheimhaltungs-, Aufbewahrungs- oder Nachweispflichten. Beispiele dafür sind:

- Produkthaftpflichtgesetz/Produktsicherheitsgesetz (Produkt muss Sicherheit bieten, die man unter Berücksichtigung aller Umstände erwarten darf)
- Geheimnisschutzpflichten (z.B. Geschäfts- und Berufsgeheimnisse, Fernmeldegeheimnis)
- Branchenspezifische Regulierungen (z.B. FINMA-Rundschreiben für Finanzbranche)
- EU-Richtlinie 2016/1148 betreffend Massnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen ("NIS-Richtlinie")

Hinweis: In der EU wurde vor kurzem ein allgemeiner "Cybersecurity Act" erlassen (in Kraft seit dem 27. Juni 2019). In diesem hat die EU ein umfassendes Zertifizierungssystem für Vertrauensgrade von IT-Security eingeführt ("grundlegend"; "werthaltig"; "hoch") um die all-

gemeine Datensicherheit in der EU zu verbessern. Aber auch diese Zertifizierungen werden auf freiwilliger Basis erfolgen.

III. GESETZLICHE ANFORDERUNGEN BZGL. DATENSCHUTZ

Das schweizerische Datenschutzgesetz (DSG) bezweckt den Schutz der Persönlichkeit sowie die Grundrechte von Personen, über die Personendaten bearbeitet werden. Konkret schreibt das DSG vor, dass Personendaten nur *rechtmässig* bearbeitet werden dürfen. Diese Bearbeitung hat nach *Treu und Glauben* zu erfolgen und muss *verhältnismässig* sein:

- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG).
- Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG).
- Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die betroffene Person die Einwilligung ausdrücklich geben (nach angemessener Information und freiwillig) (Art. 4 Abs. 5 DSG).
- Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern und Massnahmen zu treffen, damit falsche bzw. unvollständige Personendaten berichtigt bzw. vernichtet werden können (Art. 5 DSG).
- Personendaten müssen gegen unbefugtes Bearbeiten durch **angemessene technische und organisatorische Massnahmen** geschützt werden (Art. 7 DSG).

Die Bearbeiter von Personendaten sind also verpflichtet, dafür zu sorgen, dass nicht nur die eigene Datenbearbeitung rechtmässig erfolgt, sondern müssen auch *angemessene* Massnahmen treffen, damit nicht Dritte die Personendaten unrechtmässig bearbeiten können. Die Angemessenheit richtet sich dabei nach dem Stand der Technik, der Kosten, der Tragweite der Verarbeitung und der damit verbundenen Risiken für die betroffenen Personen. Als Massnahmen kommen bspw. in Frage: Pseudonymisierung und Verschlüsselung, "Privacy by Design" oder "Accountability" betreffend der getroffenen Massnahmen sowie deren Dokumentation.

Die Bearbeiter von Personendaten können ihre Systeme, Verfahren und ihre Organisation einer **Zertifizierung** durch anerkannte unabhängige Zertifizierungsstellen unterziehen (Art. 11 DSG; Verordnung über die Datenschutzzertifizierungen "VDSZ"). Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ("EDÖB") erlässt diesbezüglich entsprechende Mindestanforderungen, wobei er sich insbesondere an die Nor-

men der ISO (International Organization for Standardization) zu halten hat (Art. 4 Abs. 3 VDSZ). Der EDÖB setzt dies wie folgt um:

> *"Ein DSMS [Datenschutzmanagementsystem] genügt den Mindestanforderungen, wenn es die bestehenden internationalen Normen erfüllt, insbesondere die Norm ISO/IEC 27001:2013 (…)"* (EDÖB; Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem vom 19. März 2014)

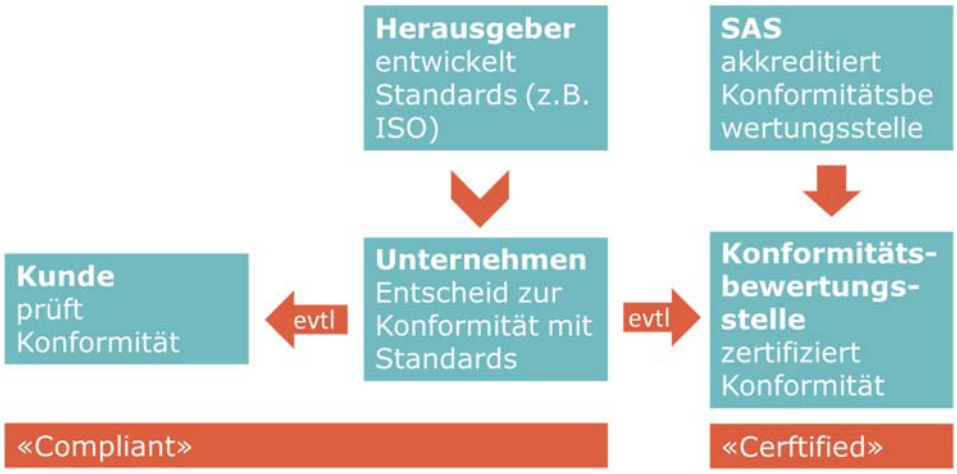
IV. IMPLEMENTIERUNG UND WIRKUNG EINES STANDARDS

Standards werden also auch von Behörden wie bspw. dem EDÖB als Richtschnur für die Einhaltung von Gesetzesbestimmungen beigezogen. Entsprechend lohnt sich ein Blick auf die Implementierung dieser Standards sowie auf die Wirkung eines basierend auf einem solchen Standard erlangten Zertifikats.

A. Implementierung eines Standards

Standards werden von diversen Organisationen, Verbänden und teilweise auch von staatlichen Stellen entwickelt. In der Regel prüfen die Herausgeber dieser Standards nicht, ob Unternehmen diese auch korrekt umsetzen. Primär akkreditieren die Herausgeber von Standards oder staatliche Stellen Dritte (sog. Konformitätsbewertungsstellen), welche die Umsetzung eines Standards in Unternehmen überprüfen und zertifizieren.

Unternehmen sind aber auch frei, sich ohne Zertifizierung an Standards zu halten und sich dann als "konform" mit einem gewissen Standard zu bezeichnen.



- Jedes Unternehmen kann sich selber als "compliant" mit einem Standard bezeichnen – nur Unternehmen, die sich tatsächlich durch eine akkreditierte Konformitätsbewertungsstelle erfolgreich zertifizieren lassen, sind "certified".

B. Wirkung eines Zertifikats

Die gesetzlichen Anforderungen betreffend Datenschutz und Datensicherheit sind abstrakt formuliert. Standards (inkl. Richtlinien, Empfehlungen etc.) können helfen, Aspekte dieser Pflichten zu konkretisieren und systematisch umzusetzen. Entsprechend geben sie zwar Hinweise dazu, was bspw. als "angemessener" Schutz betrachtet wird. Sie können aber keine abschliessende Beurteilung darüber erlauben, ob ein Unternehmen die (gesetzlich evtl. auch vertraglich) festgelegten Anforderungen in einem konkreten Fall einhält. Umgekehrt kann jedoch das Ausbleiben einer Zertifizierung einen Verstoss gegen vertragliche oder gesetzliche Pflichten bedeuten (bspw. Krankenversicherer, vgl. Art. 59a Abs. 6 KVV).

- Durch die (zertifizierte) Einhaltung eines Standards können Unternehmen erleichtert den Nachweis dafür erbringen, dass sie die notwendige Sorgfalt im den Standard betreffenden Bereich walten lassen.

V. IT-SECURITY STANDARDS UND DATENSCHUTZ

IT-Security-Standards befassen sich primär mit der Datensicherheit und nur am Rande bzw. indirekt mit Datenschutz. So wird bspw. mit der Norm ISO/IEC 27001 ein Informationssicherheits*management*system (Information Security Management System, "ISMS") zertifiziert und nicht die eigentlichen Datenverarbeitungsprozesse an sich. Damit kann ein Unternehmen mit der Umsetzung der ISO/IEC 27001 lediglich Teilaspekte eines wirksamen Datenschutzes erfüllen, z.B.:

- **Compliance**: ISO/IEC 27001 schreibt vor, dass ein Unternehmen seine regulatorischen Verpflichtungen kennen und ihre Einhaltung sicherstellen muss – insbesondere mit Bezug auf den Schutz und die Sicherheit von personenbezogenen Daten (Annex A.18.1.4).
- **Datensicherheit**: ISO/IEC 27001 verlangt eine Beurteilung der Risiken im Zusammenhang mit dem Verlust, der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie die Umsetzung von entsprechenden Massnahmen im Rahmen des ISMS (betrifft Art. 7 DSG bzw. Art. 32 DSGVO).
- **Breach Notification**: ISO/IEC 27001 verlangt, dass ein Unternehmen einen Mechanismus zur Identifikation und zum Reporting von Data Breaches erstellt (betrifft Art. 33 f DSGVO).
- **Lieferantenbeziehungen**: ISO/IEC 27001 verlangt, dass ausgelagerte Geschäftsprozesse ebenfalls kontrolliert werden und von Lieferanten Datenschutz- und Datensicherheitsmassnahmen verlangt werden (betrifft Art. 28 DSGVO).
- **Dokumentation**: ISO/IEC 27001 verlangt, dass Unternehmen wichtige Datensets identifizieren und klassifizieren (betrifft Art. 30 DSGVO).

ISO/IEC 27001 ermöglichen es einem Unternehmen somit primär, die notwendigen technischen und organisatorischen Massnahmen zu ergreifen, um Personendaten zu schützen (Art. 7 DSG bzw. Art. 32 DSGVO). Der Standard befasst sich aber nicht mit der Frage, ob die Bearbeitung von Personendaten als solche unter dem anwendbaren Recht rechtmässig bzw. verhältnismässig erfolgt.

Im August 2019 veröffentlichte nun die ISO erstmalig ein daten*schutz*-spezifisches "add-on" zur ISO/IEC 27001, die **ISO/IEC 27701:2019-08**. Das in ISO/IEC 27001 vorgeschriebene DSMS wird dabei durch ein PIMS (Privacy Information Management System) ergänzt. Mit dieser Erweiterung soll der Nachweis einer DSGVO-konformen Bearbeitung von personenbezogenen Daten *erleichtert* werden. In Annex D ermöglicht die ISO/IEC 27701 insbesondere ein "Mapping" mit Bezug auf die durch den Standard angesprochenen Bestimmungen der DSGVO. Die ISO/IEC 27701 stellt aber auch klar, dass dieses Mapping "*is purely indicative and as per this document, it is the organization's responsibility to assess its legal obligations and decide how to comply with them*". Eine Zertifizierung im Sinne von Art. 42 DSGVO, welche die Konformität mit der DSGVO belegen soll, stellt also auch dieser Standard nicht dar. Die Praxis wird zeigen, inwiefern sich Aufsichtsbehörden durch die Einhaltung dieses Standards beeindrucken lassen werden.

****