Joel Fischer / Jonas Bornhauser*

Elektronische Board Portale: Hosted in Switzerland als neuer rechtlicher Qualitätsstandard

Inhaltsübersicht

I. Einleitung

Die Digitalisierung transformiert immer weitere Bereiche des Wirtschaftslebens. Nachdem dieser Transformationsprozess insbesondere im Bereich der Social Media und des E-Shoppings begonnen hatte, erreicht er mittlerweile etwa auch die Finanzbranche (# Fintech[1]) und die Industrie (# Internet of things). Der Preis für die beträchtlichen Effizienzsteigerungen dieser Transformation ist, dass immer umfangreichere, oftmals sensitive Informationen an einem Ort lokalisiert sind, auf die mit immer effektiver werdenden technischen Mitteln zugegriffen werden kann. Die Abstimmung über das Schweizer Nachrichtendienstgesetz, die Snowden-Enthüllungen oder jüngst die Veröffentlichung gehackter E-Mails von Hillary Clinton bezeugen die wachsende Bedeutung dieser Problematik.

Im folgenden Beitrag soll dieses Spannungsverhältnis im Zusammenhang mit elektronischen Board Portalen **(«Board Portal»)** für Verwaltungsräte **(«VR»)** untersucht werden. Die Arbeit des VRs hat sich ihrerseits im Rahmen der Corporate Governance-Debatte transformiert. Dabei bestehen immer höhere Anforderungen an die Effektivität und Compliance des VRs. Board Portale können hierbei gleichzeitig ein Instrument zur Verbesserung der Corporate Governance, aber bei falscher Handhabung auch ein Compliance-Problem darstellen.

Nachfolgend werden zunächst die Funktionsweise und die Vorteile von Board Portalen erläutert. Danach werden rechtliche Fragen behandelt, welche dieses neue Instrument aufwirft. Besonderes Augenmerk wird hierbei auf die Problematik des Datenschutzes und des Zugriffs von Behörden auf Board Portal-Inhalte gelegt. Dabei zeigt sich, dass die Wahl des Standorts, an welchem diese Inhalte gespeichert bzw. gehosted werden, relevant ist für die Compliance des VRs.

---

* Joel Fischer, Master Oxford in Law and Finance, und Dr. Jonas Bornhauser, LL.M., sind Rechtsanwälte bei Bär & Karrer AG. Die Autoren danken Neil H. MacBride, Partner bei Davis Polk und ehemaliger US Attorney (zuständig für den Eastern District of Virginia), für seine Hinweise zum US Recht.

[1] Siehe zu den rechtlichen Entwicklungen hinsichtlich der Finanzbranche (insbesondere im Bereich Fintech) den Artikel von Tina Balzli/Joel Fischer im International Financial Law Review Magazine, Februar 2017.

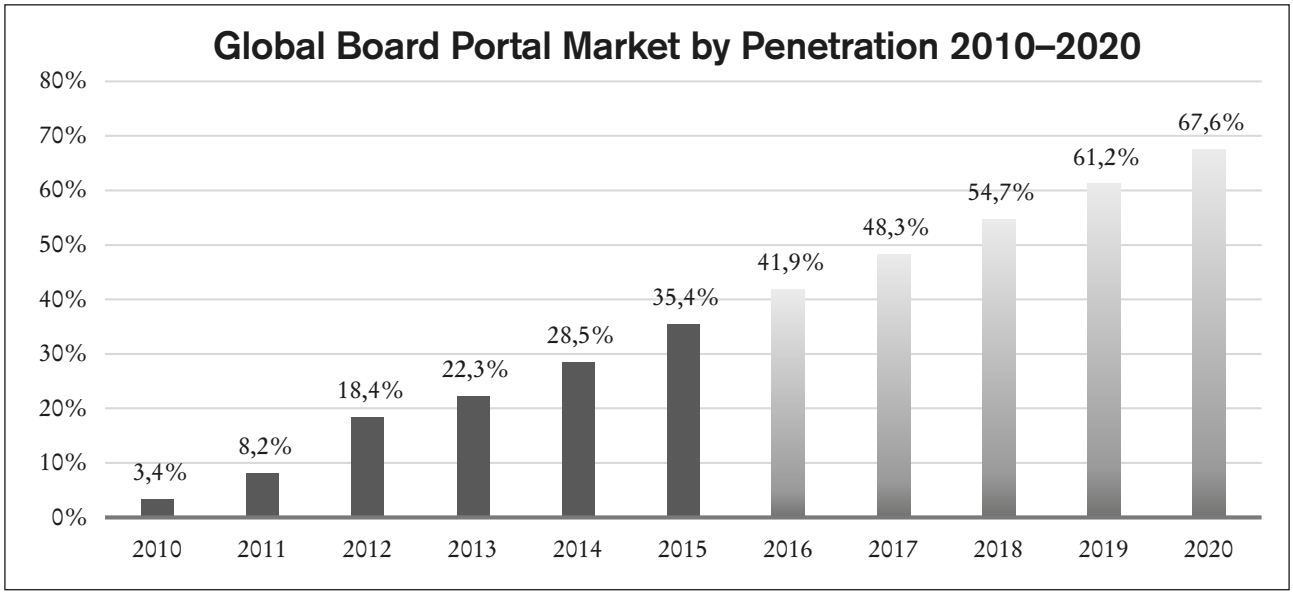

Abbildung 1: Quelle: Dadael Research, 19

II. Elektronische Board Portale als neues Instrument zur Effizienzsteigerung der VR-Arbeit

1. Vorteile von Board Portalen

Board Portale ermöglichen VR-Mitgliedern, jederzeit auf Sitzungsunterlagen und weitere Informationen elektronisch zuzugreifen. In der Regel werden die Informationen hierbei auf einer App oder einer Webseite per Tablet-Computer, Smartphones oder PCs online zur Verfügung gestellt.[2]

Traditionell wurden VR-Unterlagen per Post oder E-Mail versandt. Diese Formen der Übermittlung haben verschiedene Nachteile. Bei der Zustellung per Post geht oft wertvolle Zeit für die Übermittlung der Informationen verloren. Grundsätzlich besteht ein Zielkonflikt zwischen dem Bedürfnis, dass die Informationen möglichst aktuell sind und dass der VR trotzdem genügend Zeit hat, die Unterlagen sorgfältig zu studieren. Hierbei ist das Management oft daran interessiert, die Sitzungsunterlagen dem VR aus Zeitgründen möglichst spät zuzustellen, während der VR die Unterlagen möglichst frühzeitig erhalten möchte. Angesichts dieser Problematik scheint es anachronistisch, noch zusätzlich Zeit nur für die Zustellung zu verschwenden (vor allem in einem international zusammengesetzten VR). Die Zusendung in Papierform führt ferner dazu, dass viele Kopien im Umlauf sind, was die Gefahr von Indiskretionen erhöht.

Ausserdem ist es viel praktischer für Verwaltungsräte, die oft sehr umfangreichen Unterlagen elektronisch auf dem Tablet einzusehen, ohne (z.B. auf Reisen) Aktenberge «rumschleppen» zu müssen.

Der Transfer über verschlüsselte E-Mails ist sicher, aber auch hier stellen sich analoge Probleme, wenn die Unterlagen ausgedruckt werden. Oft werden auch keine verschlüsselten E-Mails benutzt, da diese aufwändig und mässig verbraucherfreundlich sind.

Board Portale entwickeln sich ferner stetig weiter und bieten vermehrt zusätzliche Dienstleistungen an. So bieten gewisse Plattformen «Board Calendars» an, welche alle VR-Sitzungen und sonstige relevanten VR-Termine enthalten und das Aufsetzen einer VR-Sitzung erleichtern. Teilweise bestehen auch eigene spezielle Kommunikationsmittel für den Board (E-Mail, Chat etc.) und Funktionen für Abstimmungen (Voting Tools) oder sonstigen Input von VR-Mitgliedern (z.B. Selbstevaluation des VRs). Schlussendlich besteht auch ein durchsuchbares Archiv mit vergangenen Sitzungsunterlagen und weiteren Kerninformationen (z.B. Statuten und Organisationsreglement, Jahresberichte).[3]

Summa summarum ermöglichen Board Portale, die Informationsverarbeitung und Kommunikation im VR deutlich effizienter zu gestalten. Dies ist nicht zuletzt hinsichtlich der *gesteigerten Anforderungen an das Informationsniveau von VRs* im Rahmen der Corporate Governance-Debatte von grossem Wert.[4]

---

[2] Vgl. Daedal Research, Global Board Portal Market: Trends & Opportunities (2016 Edition), Februar 2016, 7 ff., abrufbar unter <www.marketreportsonline.com/445165-toc.html> (zuletzt besucht am 18. November 2016).

[3] Vgl. Daedal Research (FN 2), 10 f.

[4] Siehe hierzu Joel Fischer, Information und Verantwortlichkeit von Verwaltungsräten, Diss. Bern (erscheint in Kürze).

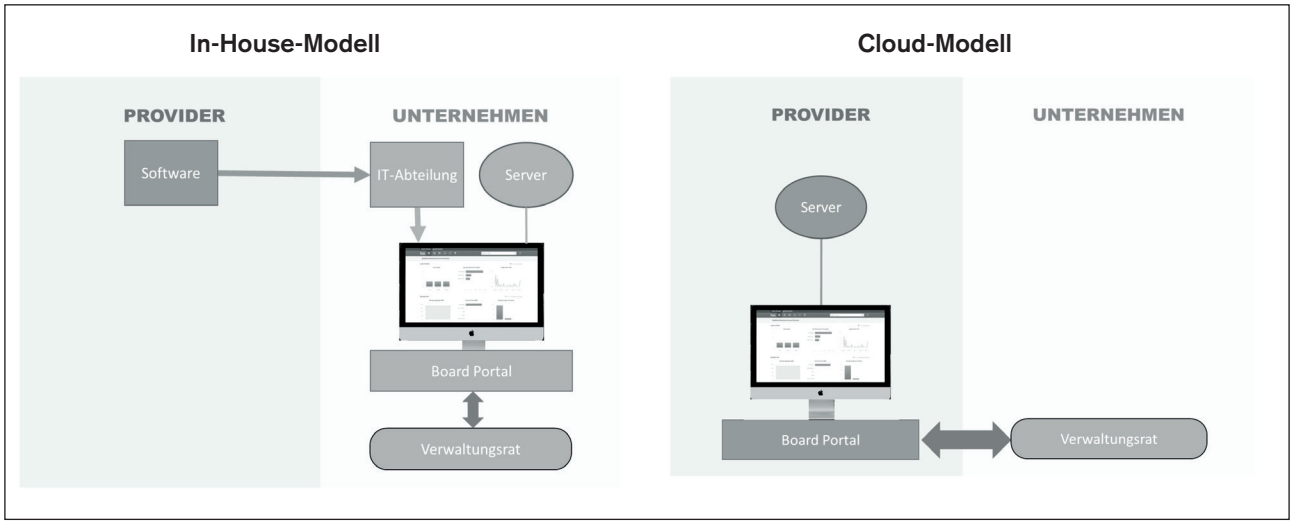

Abbildung 2: Quelle: eigene Darstellung

2. Zunehmende Verbreitung

Die Verbreitung von Board Portalen hat in den letzten Jahren deutlich zugenommen. Zu Beginn war dies noch eine Extravaganz von besonders technik-affinen VR-Mitgliedern. Noch im Jahre 2010 ging man von einer Marktpenetration von 3,4 % weltweit aus.[5] Mittlerweile sind es bereits 35,4 % und Schätzungen gehen davon aus, dass dieser Wert bis 2020 auf ca. 68 % anwachsen wird.[6] Nicht zuletzt das Aufkommen von Tablets, insbesondere iPads, hat die Verbreitung von Board Portalen deutlich beschleunigt. Anstelle von sperrigen Laptops können die Informationen nun auf handlichen Tablets eingesehen werden.

3. Funktionsweise von Board Portalen

Es bestehen verschiedene Modelle für die Funktionsweise von Board Portalen:

Zunächst ist es möglich, dass das Unternehmen eine entsprechende Software kauft oder gar selbst entwickelt und diese dann auf den eigenen Servern installiert (In-House-Modell). Eine andere Möglichkeit ist es, dass das Board Portal vollumfänglich von einem externen Provider **(«Board Portal Provider»)** angeboten wird. Die VR-Mitglieder haben dann in der Regel über das Internet Zugang auf das Board Portal (Cloud-Modell).

Beim In-House-Modell befinden sich die Daten meistens auf den Servern des Unternehmens, während die Daten beim Cloud-Modell auf den Servern des Board Portal Providers (oder dessen Subunternehmer) gespeichert sind.

Das Cloud-Modell ist mit Abstand am weitesten verbreitet. Schätzungen gehen davon aus, dass ca. 90 % der Board Portale das Cloud-Modell verfolgen.[7] Die nachfolgenden rechtlichen Ausführungen beschränken sich deshalb auf das Cloud-Modell. Es sei aber darauf hingewiesen, dass je nach Ausgestaltung[8] gewisse der hier erwähnten Risiken beim In-House-Modell nicht relevant sind. Dieses hat aber andere gewichtige Nachteile. Eine In-House-Lösung ist deutlich teurer und bindet Ressourcen des eigenen Unternehmens. Die In-House-Lösung erlaubt zwar in der Theorie eine Anpassung an die individuellen Bedürfnisse des Unternehmens; oft funktioniert die In-House-Lösung aber weniger gut als die Portale von spezialisierten Providern. Ausserdem besteht hier die Gefahr, dass Personen aus dem Unternehmen Informationen einsehen, welche der VR unter Verschluss halten möchte oder muss. Wenn der VR zum Beispiel die Zukunft des CEOs behandelt, sollte sichergestellt werden, dass dieser keine Einsicht in die entsprechenden Unterlagen erhält.[9] Wenn der Server aber «In-House» ist, besteht die Gefahr, dass der CEO den zuständigen IT-Mitarbeiter informell kontaktiert und Einsicht verlangt. Der IT-Mitarbeiter gelangt so in ein Dilemma und wird nicht selten dem CEO die Informationen unter der Hand beschaffen. Noch heikler ist der Fall, wenn etwa Einsparungen bei der IT-Abteilung selber beschlossen werden und die betroffenen Mitarbeiter die Daten bereits auf dem Sever einsehen können.

---

5 Daedal Research (FN 2), 19.

6 Daedal Research (FN 2), 19 f.

7 Daedal Research (FN 2), 20.

8 Oft werden die notwendigen Serverkapazitäten von Dritten gemietet (sog. private cloud). Wenn diese private cloud z.B. in der USA ist, dann stellen sich die gleichen Probleme wie bei einem US Board Portal Provider.

9 Auch andere Personen sollten keine Einsicht haben, z.B. wegen *ad hoc*-Regeln, Insidernormen oder Geheimhaltungsvereinbarungen mit Dritten.

Wie nachfolgend eingehender erörtert wird, ist es für die rechtliche Beurteilung der Board Portale von grosser Bedeutung, wo der Server steht. Ferner ist auch relevant, wo sich der Sitz des Board Portal Providers und derjenige der das Board Portal nutzenden Gesellschaft **(«Gesellschaft»)** befindet.

III. Gesellschaftsrechtliche Aspekte

Aus gesellschaftsrechtlicher Sicht ist die Zulässigkeit von Board Portalen unproblematisch, wenn diese als Unterstützung von VR-Sitzungen dienen, bei welchen die VR-Mitglieder physisch anwesend sind. Board Portale können aber auch zur Meinungsbildung ausserhalb von physisch abgeschalteten VR-Sitzungen benutzt werden, etwa im Rahmen der Chat- oder E-Mail-Funktion des Board Portals. Eine weitere mögliche Kommunikationsform wären Video- oder Telefonkonferenzen unter simultaner Einblendung der Präsentation. Diese Funktion ist heute i.d.R. noch nicht in Board Portalen enthalten, aber es liegt nahe, dass dies in Zukunft auch angeboten wird. Es soll daher auch auf diese Kommunikationsform eingegangen werden.

Im gesetzgeberischen Leitbild wird davon ausgegangen, dass die Beschlüsse des VRs primär im Rahmen einer mündlichen Beratung gefasst werden. Nach Art. 713 Abs. 2 OR ist auch eine schriftliche Zustimmung zu einem Antrag möglich, sofern kein Mitglied eine mündliche Beratung verlangt. Es fragt sich, wie diese Bestimmung hinsichtlich der alternativen Formen der Beschlussfassung bei Board Portalen auszulegen ist.

1. Video- und Telefonkonferenzen

Die herrschende Lehre betrachtet Video- oder Telefonkonferenzen als zulässig.[10] Jedoch wird immer wieder gemahnt, dass diese nur mit Zurückhaltung, insbesondere bei besonderer Dringlichkeit, durchzuführen sind.[11]

Unseres Erachtens ist der herrschenden Lehre zuzustimmen, dass diese Sitzungsformen grundsätzlich zulässig sind. Allerdings müssen die Voraussetzungen geschaffen werden, dass alle Mitglieder dem Geschehen folgen und sich an der Willensbildung beteiligen können.[12] Hierfür muss etwa die technische Durchführung gewährleistet sein (z.B. ausreichender Telefonempfang) und die Mitglieder sind, falls möglich, vorab angemessen zu orientieren.[13] Ferner sollten den VR-Mitgliedern die massgeblichen Unterlagen während der Sitzung zur Verfügung stehen, damit sie der Beratung folgen können.[14] Bei Konferenzen mittels Board Portalen kann dies relativ einfach sichergestellt werden.

Es fragt sich ferner, ob jedes VR-Mitglied analog zu Art. 713 Abs. 2 OR verlangen kann, dass anstelle einer Video- oder Telefonkonferenz eine Beratung stattfinden muss, bei der die VR-Mitglieder physisch anwesend sind. Dies ist nach der herrschenden Lehre nicht der Fall.[15]

Unseres Erachtens ist hier entscheidend, ob solche alternativen Verhandlungsformen unter den Begriff der mündlichen Beratung nach Art. 713 Abs. 2 OR subsumiert werden können. Videokonferenzen kommen der Beratung mit physischer Anwesenheit sehr nahe. Diese erlauben, gleich wie bei einer Sitzung mit physischer Anwesenheit, dass die VR-Mitglieder interagieren, Argumente diskutieren und gemeinsam eine Meinung bilden. Hierbei können die Mitglieder jeweils auch die Mimik und Gestik der anderen Mitglieder sehen, was die Willensbildung und die Kommunikation auf der Metaebene zusätzlich erleichtert. Solche Formen der Informationsvermittlung, werden in der Kommunikationsforschung als «reiche» Medien bezeichnet.[16]

Da Videokonferenzen all die Vorteile einer Beratung mit physischer Anwesenheit weitgehend abdecken, sind diese unseres Erachtens in einer zeitgemäss-teleologischen Auslegung unter die mündliche Beratung nach Art. 713 Abs. 2 OR zu subsumieren.

Telefonkonferenzen sind ein «ärmeres» Medium als Videokonferenzen, da Mimik und Gestik nicht einsehbar

---

10 Peter Böckli, Schweizer Aktienrecht, 4. Aufl., Zürich/Basel/Genf, 2009, § 13 N 136 f. m.w.H.; Peter Forstmoser, Organisation und Organisationsreglement der Aktiengesellschaft – Rechtliche Ordnung und Umsetzung in der Praxis, Zürich/Basel/Genf, 2011, § 11 N 13; ZK OR-Homburger, Art. 713 OR N 298 f.; Ivo Hungerbühler, Der Verwaltungsratspräsident, Diss. Zürich, 2003, 101 f. m.w.H. (= SSHW 219); Georg Krneta, Verwaltungsrat, Praxiskommentar, Art. 707–726, 754 OR und Spezialgesetze, 2. Aufl., Bern 2005, N 829; Roland Müller/Lorenz Lipp/Adrian Plüss, Der Verwaltungsrat – Ein Handbuch für Theorie und Praxis, 4. Aufl., Zürich, 2014, 274; Hans Caspar von der Crone, Aktienrecht, Bern, 2014, § 4 N 124 f.; Rolf Watter/Sebastian Flückiger, Beschlussfassung unter abwesenden VR-Mitgliedern (inkl. durch Zirkularbeschluss), GesKR 2015, 411 ff. m.w.H.

11 So etwa Böckli (FN 10), § 13 N 136a ff. m.w.H.; Krneta (FN 10), N 829; ZK OR-Homburger, Art. 713 OR N 298 f.

12 Vgl. Hungerbühler (FN 10), 102.

13 Krneta (FN 10), N 827. Insbesondere sollten die Unterlagen wenn möglich vorgängig verschickt werden. Ausnahmsweise kann bei grosser Dringlichkeit hierauf verzichtet werden, siehe hierzu Böckli (FN 10), § 13 N 210 ff.; Fischer (FN 4), § 13 A. III m.w.H.

14 Böckli (FN 10), § 13 N 136.; vgl. auch Hungerbühler (FN 10), 102.

15 Böckli (FN 10), § 13 N 136a ff. m.w.H.; Forstmoser (FN 10) § 11 N 13; Hungerbühler (FN 10), 101 f.; Krneta (FN 10), N 829; Müller/Lipp/Plüss (FN 10), 274. Differenzierend: von der Crone (FN 10), § 4 N 124 f.; Watter/Flückiger (FN 10), 411 ff. A.M. ZK OR-Homburger, Art. 713 OR N 298 f.

16 Beide Medien zeichnen sich dadurch aus, dass sie zeitnah Interaktion erlauben und verschiedene Kommunikationskanäle, wie Mimik und Gestik umfassen, siehe hierzu und der Kommunikation im VR allgemein Fischer (FN 4), § 5 C. I. m.w.H.

sind.[17] Diese erlauben aber trotzdem, dass ein interaktiver Meinungsaustausch stattfindet. Sie sind daher unseres Erachtens auch unter dem Begriff der «mündlichen Beratung» zu subsumieren. Dies gilt umso mehr, als im OR nicht explizit steht, dass die Mitglieder physisch anwesend sein müssen und der Wortlaut somit prinzipiell Telefonkonferenzen einschliesst. Dies scheint im Übrigen auch zweckmässig. Telefonkonferenzen werden i.d.R. bei grosser Dringlichkeit einberufen. Auch bei einer gewissen Dringlichkeit ist es i.d.R. sinnvoll, dass jedes VR-Mitglied das Recht hat, eine Beratung einzufordern, in der es seine Argumente im Gremium vorbringen kann. Hierfür reicht allerdings eine Telefonkonferenz. Wenn aber eine physische Sitzung abgehalten werden müsste, besteht gerade bei dringlichen Angelegenheiten die Gefahr, dass die Einberufung der Sitzung zu lange dauern würde. Ein VR-Mitglied könnte dies dazu missbrauchen, um den dringend erforderlichen Entscheid zu verzögern und letztlich hinfällig werden zu lassen.[18] Ein interessanter Ansatz ist auch, ein entsprechendes «Vetorecht» nur dann zu gewähren, wenn diese alternativen Sitzungsformen keine Grundlage im Organisationsreglement haben.[19] Unseres Erachtens ist eine entsprechende Grundlage im Organisationsreglement auf jeden Fall zu empfehlen; diese ist allerdings nicht notwendig, da die alternativen Sitzungsformen bereits unter den Begriff der mündlichen Beratung subsumiert werden können, womit das Vetorecht entfällt.

Bei Telefonkonferenzen ist besonders wichtig, dass die Mitglieder, welche sich telefonisch einwählen, die Unterlagen vor sich haben und nachvollziehen können, auf welche Folie der Vortragende sich gerade bezieht. Dies können Board Portale erleichtern, indem sie dem Vortragenden ermöglichen zu bestimmen, welche Folien auf dem Device der Teilnehmer angezeigt werden.

2. E-Mail-Ketten und Chat

Eine weitere Möglichkeit ist die Abstimmung über E-Mails oder eine Chatfunktion innerhalb des Board Portals.[20]

E-Mails und Chats sind klarerweise keine Formen der mündlichen Beratung.[21] Es findet zwar Interaktion statt, diese erfolgt aber über den Schriftverkehr. Auch wenn man argumentieren könnte, dass eine Beratung auch per Chat möglich wäre, so verbietet der klare Wortlaut eine Subsumtion unter den Begriff der *mündlichen* Beratung. Ausserdem gehen hier neben Mimik und Gestik zusätzlich auch der Tonfall als Mittel der Kommunikation verloren.

Liegt keine mündliche Beratung vor, so sind die Entscheide nach Art. 713 Abs. 2 OR auf dem Zirkularweg zu treffen. Die Voraussetzungen hierfür sind die Schriftlichkeit des Beschlusses und dass jedes VR-Mitglied die Möglichkeit erhält, eine mündliche Beratung zu verlangen.[22] Wenn ein VR-Mitglied eine Beratung verlangt, so muss diese vorgenommen werden,[23] womit jedes VR-Mitglied *de facto* ein Vetorecht gegen einen Zirkularbeschluss hat.[24]

Hinsichtlich des Erfordernisses der Schriftlichkeit finden nach herrschender Lehre[25] die Vorschriften in Art. 12 ff. OR Anwendung. Danach muss in Anwendung von Art. 13 OR jede Person den Beschluss unterzeichnen. Dem ist gemäss Art. 14 Abs. 2bis OR die elektronische Signatur gleichgestellt. Es wird hierbei von der herrschenden Lehre auch als ausreichend betrachtet, wenn das VR-Mitglied einen Papierausdruck erstellt, den es unterschreibt und dann wiederum einscannt und per E-Mail zurücksendet.[26] Es ist aber genau nicht die Idee eines Board Portals, dass Papierausdrücke erstellt werden. Falls dies noch nicht der Fall ist, sollten die Board Portale (in der Schweiz) künftig die Möglichkeit bieten, integriert im System ohne grossen Aufwand eine elektronische Signatur hinzuzufügen.

Ferner ist wichtig, dass klar ist, welchem Beschlusstext zugestimmt wird. Dies kann am besten erreicht werden, wenn eine Person den entsprechenden Beschluss nochmals festhält, während alle anderen per elektronischer Signatur zustimmen.

Eine Lehrmeinung[27] plädiert dafür, dass man im Organisationsreglement die Möglichkeit einräumen kann, per E-Mails (oder vergleichbaren Methoden) einen Beschluss zu fassen, ohne dass eine elektronische Signatur oder eine Unterschrift auf einem gescannten Dokument notwendig ist. Auch wenn diese Meinung einiges für sich hat, ist die Unterschrift nach herrschender Lehre

---

17 Eine weitere Problematik stellt sich hinsichtlich der Identifikation der Teilnehmenden, da diese nur über die Stimme schwerer möglich ist.

18 Watter/Flückiger (FN 10), 412, verweisen in diesem Kontext zu Recht auf das Rechtsmissbrauchsverbot.

19 Watter/Flückiger (FN 10), 412.

20 Analoge Überlegungen gelten bei «Voting-Buttons».

21 Vgl. Hungerbühler (FN 10), 102.

22 Da keine Beratung stattfindet, muss der Antrag ferner so formuliert sein, dass die anderen Personen zustimmen oder ablehnen können, vgl. ZK OR-Homburger, Art. 713 OR N 331.

23 Vgl. Böckli (FN 10), § 13 N 139; BSK OR II-Wernli/Rizzi, Art. 713 N 23.

24 Es ist allerdings keine Einstimmigkeit erforderlich. So kann ein VR-Mitglied etwa implizit oder explizit auf die Einberufung einer Beratung verzichten, sich aber der Stimme enthalten oder den Antrag ablehnen, vgl. von der Crone (FN 10), § 4 N 123.

25 Implizit Böckli (FN 10), § 13 N 138; Forstmoser (FN 10), § 11 N 21; ZK OR-Homburger, Art. 713 OR N 331; Krneta (FN 10), N 815; a.M. Watter/Flückiger (FN 10), 414 ff.; BSK OR II-Wernli/Rizzi, Art. 713 N 19.

26 BSK OR II-Wernli/Rizzi, Art. 713 N 19; Forstmoser (FN 10), § 11 N 21; Reto Sutter/Nicolas Fancini, Zirkularbeschlüsse des Verwaltungsrates, TREX 2014, 106; Watter/Flückiger (FN 10), 413; vgl. auch Böckli (FN 10), § 13 N 138.

27 Watter/Flückiger (FN 10), 414 ff.

wohl zwingend notwendig.[28] Es ist daher zu empfehlen, dass die Zustimmung der VR-Mitglieder (elektronisch) unterzeichnet wird. Sofern dies aber nicht erfolgt, ist unseres Erachtens zumindest bei einem Board Portal der Beschluss nicht ungültig. VR-Beschlüsse sind nicht anfechtbar,[29] können aber bei klaren Verstössen nichtig sein. Die Schwelle für die Nichtigkeit ist hierbei im Gesellschaftsrecht nach herrschender Lehre und Rechtsprechung ausserordentlich hoch.[30] Diese Zurückhaltung ist sachgerecht, da ein übermässiger Eingriff in die Willensbildung des VRs die Handlungsfähigkeit der Gesellschaft gefährden könnte.[31] Die *ratio legis* des Unterschriftserfordernisses liegt darin, dass der Sender identifizierbar ist.[32] Theoretisch könnte bei E-Mails oder Chats die Gefahr bestehen, dass sich eine andere Person einloggen und das E-Mail abschicken würde. Diese Gefahr ist aber bei Board Portalen besonders gering. Beim Einloggen in ein Board Portal bestehen typischerweise sehr hohe Anforderungen an die Identifikation. Die Identität des Absenders ist somit bei Board Portalen i.d.R. sogar eher besser sichergestellt als bei einer Unterschrift oder Telefonkonferenz, bei der man die Person lediglich an der Stimme erkennt.[33] Selbst wenn man nun annimmt, dass eine Unterschrift erforderlich ist, läge daher unseres Erachtens kein so «krasser» formeller Mangel[34] vor, dass die Nichtigkeit des Beschlusses gerechtfertigt wäre.[35] In jedem Fall ist es aber empfehlenswert, im Organisationsreglement die Beschlussfassung mittels der Funktionalitäten innerhalb des Board Portals bzw. mittels E-Mail, Chat etc. vorzusehen.[36]

3. Änderungen gemäss dem Entwurf zur Aktienrechtsrevision 2016

Der Bundesrat hat am 23. November 2016 die Botschaft zur Revision des Aktienrechts zuhanden des Parlaments verabschiedet. Darin finden sich auch angepasste Bestimmungen zur Beschlussfassung mittels elektronischen Mitteln. Art. 713 Abs. 2 des E-OR lautet:

«Art. 713 Abs. 2

[2] Der Verwaltungsrat kann seine Beschlüsse fassen:

1. an einer Sitzung mit Tagungsort;
2. unter Verwendung elektronischer Mittel gemäss den Artikeln 701c–701e;
3. auf schriftlichem Weg auf Papier oder in elektronischer Form, sofern sämtliche Mitglieder ihre Zustimmung zur Art der Beschlussfassung erteilt haben.»[37]

Art. 701c–701e E-OR beziehen sich grundsätzlich auf die Verwendung elektronischer Mittel an der GV und lauten folgendermassen:[38]

«Art. 701c

Der Verwaltungsrat kann vorsehen, dass Aktionäre, die nicht am Ort der Generalversammlung anwesend sind, ihre Rechte auf elektronischem Weg ausüben können.

Art. 701d

[1] Eine Generalversammlung kann mit elektronischen Mitteln ohne Tagungsort durchgeführt werden, wenn die Statuten dies vorsehen und der Verwaltungsrat in der Einberufung einen unabhängigen Stimmrechtsvertreter bezeichnet.

[2] Bei Gesellschaften, deren Aktien nicht an einer Börse kotiert sind, kann der Verwaltungsrat auf die Bezeichnung eines unabhängigen Stimmrechtsvertreters verzichten, sofern alle Aktionäre damit einverstanden sind.

Art. 701e

[1] Der Verwaltungsrat regelt die Verwendung elektronischer Mittel.

[2] Er stellt sicher, dass:

1. die Identität der Teilnehmer feststeht;
2. die Voten in der Generalversammlung unmittelbar übertragen werden;
3. jeder Teilnehmer Anträge stellen und sich an der Diskussion beteiligen kann;
4. das Abstimmungsergebnis nicht verfälscht werden kann.»

Art. 713 Abs. 2 Ziff. 3 des Entwurfs betrifft, neben Beschlüssen in Papierform, insbesondere auch E-Mails.[39] Diese Bestimmung ist wohl so zu interpretieren, dass bei E-Mails keine eigenhändige bzw. elektronische Unterschrift notwendig ist. Der Gesetzeswortlaut ist diesbezüglich aber nicht ganz eindeutig.[40] Unseres Erachtens sollte die Bestimmung so formuliert werden, dass klar ist, dass bei E-Mails keine Unterschrift erforderlich ist.

---

28 BSK OR II-Wernli/Rizzi, Art. 713 N 19; Böckli (FN 10), § 13 N 138; Forstmoser (FN 10), § 11 N 21; Krneta (FN 10), N 815; ZK OR-Homburger, Art. 713 OR N 331; a.M. Watter/Flückiger (FN 10), 414 ff.

29 Böckli (FN 10), § 13 N 264 ff. m.w.H.

30 BSK OR II-Wernli/Rizzi, Art. 714 N 10; Böckli (FN 10), § 13 N 278; Müller/Lipp/Plüss (FN 10), 332; BGE 137 III 465; BGE 115 II 474.

31 Vgl. Fischer (FN 4), § 9 B. V. 1. m.w.H.

32 Böckli (FN 10), § 13 N 138; BSK OR II-Wernli/Rizzi, Art. 713 N 19; Krneta (FN 10), N 815; Sutter/Fancini (FN 10), 107; Christian Kunz, Werben um Aktionärsstimmen bei Schweizer Publikumsgesellschaften («Proxy Fights»), Diss. Zürich 2015, 144 f. (= ZStP 264).

33 Vgl. Watter/Flückiger (FN 10), 414 ff.

34 Vgl. Böckli (FN 10), § 13 N 275.

35 Vgl. hierzu die Ausführungen in Watter/Flückiger (FN 10), 414 ff.; eher a.M. BSK OR II-Truffer/Dubs, Art. 706b N 17 ff.

36 So auch Müller/Lipp/Plüss (FN 10), 273.

37 Entwurf zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/entw-d.pdf> (zuletzt besucht am 24. November 2016), 35.

38 Entwurf zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/entw-d.pdf> (zuletzt besucht am 24. November 2016), 32.

39 Erfasst sind wohl auch Chats.

40 Man könnte den Wortlaut so interpretieren, dass sich der «schriftliche Weg», und damit womöglich auch das Unterschriftserfordernis, nicht nur «auf Papier», sondern auch auf die «elektronische Form» bezieht.

Das Vetorecht bleibt bei dieser Form der Beschlussfassung bestehen. Da bei E-Mails keine Beratung stattfinden kann, ist ein Vetorecht auch durchaus angebracht. Wenn ein Mitglied sich gegen die Beschlussfassung per E-Mail ausspricht, kann die Beratung relativ unkompliziert per Telefon- oder Videokonferenz stattfinden (siehe nachfolgend).

Art. 713 Abs. 2 Ziff. 2 E-OR bezieht sich insbesondere auf die Beschlussfassung mittels Video- und Telefonkonferenz.[41] Voraussetzung für die Verwendung elektronischer Mittel ist gemäss Art. 701e Abs. 2 E-OR i.V.m. Art. 713 Abs. 2 Ziff. 2 E-OR, dass

- die Identität der Teilnehmer feststeht;
- die Voten unmittelbar übertragen werden;
- jeder Teilnehmer Anträge stellen und sich an der Diskussion beteiligen kann;
- das Abstimmungsergebnis nicht verfälscht werden kann.

Dies kann zweifelsohne mittels Videokonferenz gewährleistet werden. Unseres Erachtens reicht auch die Interaktion im Rahmen einer Telefonkonferenz.[42] Ein Vetorecht besteht bei dieser Beschlussform nicht. Ein solches Vetorecht wäre auch nicht angebracht. Bei Video- und Telefonkonferenzen kann ein genügender Austausch stattfinden. Die Gefahr eines Missbrauchs des Vetorechts durch einzelne VR-Mitglieder überwiegt hier den Vorteilen des Vetorechts.[43]

Der pauschale Verweis auf Art. 701c–701e E-OR, welche die Beschlussfassung an der GV betreffen, ist unseres Erachtens unglücklich. Diese Artikel unterscheiden, ob die GV gesamthaft virtuell stattfindet (virtuelle GV) oder ob die GV an einem bestimmten Ort tagt und gewisse Aktionäre sich zusätzlich zuschalten lassen können.[44] Wenn sich die Aktionäre nur zuschalten, reicht ein Beschluss des VRs. Bei einer virtuellen GV ist hingegen eine Grundlage in den Statuten notwendig. Übertragen auf den VR würde dies bedeuten, dass neuerdings eine Statutengrundlage notwendig wäre für eine virtuelle VR-Sitzung. Dies ist unseres Erachtens nicht sachgerecht und widerspricht der Konzeption des Aktienrechts: Der Modus der Beschlussfassung gehört eindeutig zu den Vorgängen, welche der VR unabhängig von der GV bzw. den Statuten regeln können sollte. Ausserdem organisiert sich der VR nach herrschender Lehre (mit wenigen Ausnahmen[45]) zwingend selbst.[46] Dementsprechend sollte der Entwurf geändert werden, damit klar hervorgeht, dass bei virtuellen VR-Sitzungen keine Grundlage in den Statuten notwendig ist.[47] Es ist dagegen sinnvoll, wenn der VR die Einzelheiten der elektronischen Beschlussfassung im Organisationsreglement regelt (vgl. 716b Abs. 2 Ziff. 1 E-OR).[48] Die Bedürfnisse können je nach VR durchaus variieren. So ist die Situation bei einem VR, bei dem die Mitglieder über die ganze Welt verstreut sind, nicht die gleiche wie bei einem lokalen VR, bei dem alle Mitglieder in der gleichen Stadt wohnen. Dem VR sollte daher ein möglichst grosser Handlungsspielraum gewährt werden.

Schlussendlich kann auch das Erfordernis der Stimmrechtsvertreter in Art. 701d E-OR für den VR keine Anwendung finden.

Aufgrund der obigen Ausführungen schlagen wir vor Art. 713 Abs. 2 OR folgendermassen zu modifizieren:

«Art. 713 Abs. 2

[2] Der Verwaltungsrat kann seine Beschlüsse fassen:

1. an einer Sitzung mit Tagungsort;
2. unter Verwendung elektronischer Mittel, **sofern die Voraussetzungen gemäss Art. 701e Abs. 2 erfüllt sind;**
3. auf schriftlichem Weg auf Papier oder in elektronischer Form, sofern sämtliche Mitglieder ihre Zustimmung zur Art der Beschlussfassung erteilt haben. **Die Zustimmung in elektronischer Form bedarf keiner Unterschrift gemäss Art. 14.**

IV. Datenschutzrechtliche Vorgaben

Wenn eine Gesellschaft einen Board Portal Provider nutzt, ist davon auszugehen, dass dabei Personendaten bearbeitet werden und deshalb datenschutzrechtliche Grundsätze Anwendung finden. Wird einer der zahlreichen Board Portal Provider ausserhalb der Schweiz gewählt, geht die Nutzung des Board Portals zudem mit der Übermittlung («Bekanntgabe») von Personendaten ins Ausland einher, was zusätzliche datenschutzrechtliche Implikationen nach sich zieht. Darauf ist im Folgenden genauer einzugehen.

---

41 Botschaft zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/bot-d.pdf> (zuletzt besucht am 24. November 2016), 169 f.

42 So auch die Botschaft zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/bot-d.pdf> (zuletzt besucht am 24. November 2016), 169 f.

43 Siehe Ziffer III. 1.

44 Botschaft zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/bot-d.pdf> (zuletzt besucht am 24. November 2016), 160 f.

45 Siehe etwa Art. 626 Abs. 2 E-OR, Art. 712 Abs. 2 und Abs. 4 E-OR sowie im Bereich der Vergütung Art. 733 ff. E-OR. Es fällt auf, dass diese Ausnahmen im Entwurf des Bundesrates bzw. teilweise bereits in der VegüV ausgebaut wurden.

46 Forstmoser (FN 10) § 8 N 31, § 11 N 5 m.w.H.; von der Crone (FN 10), § 4 N 65; Krneta (FN 10), N 1220 m.w.H.

47 Auch ist eine Differenzierung, ob eine Sitzung völlig virtuell oder unter Beischaltung einzelner VR-Mitglieder stattfindet, beim VR nicht angebracht.

48 Vgl. auch Botschaft zur Änderung des Obligationenrechts (Aktienrecht), undatiert, abrufbar unter <www.ejpd.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/aktienrechtsrevision14/voabzockerei/bot-d.pdf> (zuletzt besucht am 24. November 2016), 170 in welcher aber wiederum systemwidrig auch auf die Statuten verwiesen wird.

1. Datenbearbeitung in der Schweiz

1.1 Räumliche Anwendbarkeit schweizerischen Datenschutzrechts

Das schweizerische Datenschutzrecht umfasst zivilrechtliche, öffentlich-rechtliche und strafrechtliche Bestimmungen, die je eigenen kollisionsrechtlichen Regelungen unterliegen.[49] Die nachfolgenden Ausführungen befassen sich primär mit den zivilrechtlichen Bestimmungen. Daneben wird auf die Bestimmungen öffentlich-rechtlicher Natur soweit eingegangen, wie diese die Bekanntgabe von Personendaten ins Ausland zum Gegenstand haben.

Wenn eine Gesellschaft ein Board Portal nutzt, werden regelmässig Personendaten bearbeitet, und zwar sowohl von der Gesellschaft wie auch vom Board Portal Provider.[50] Dies zieht dann die Anwendbarkeit schweizerischen Datenschutzrechts nach sich,[51] wenn die Datenbearbeitung in der Schweiz erfolgt. Von einer Datenbearbeitung in der Schweiz ist im vorliegenden Zusammenhang dann auszugehen, wenn die Personendaten von einer Gesellschaft mit Sitz in der Schweiz erhoben werden. Ob das vom Provider gehostete Board Portal auf einem Server betrieben wird, der in den Räumlichkeiten der Gesellschaft steht (In-House-Modell) oder extern, beispielsweise auf einem Server des Board Portal Providers (Cloud-Modell), ist nicht relevant; in beiden Fällen kommt schweizerisches Datenschutzrecht und damit insbesondere die allgemeinen Datenbearbeitungsgrundsätze gemäss Art. 4 DSG zur Anwendung. Dies gilt selbst dann, wenn sich der Serverstandort ausserhalb der Schweiz befindet. Wie nachfolgend dargelegt, stellen sich aus datenschutzrechtlicher Sicht beim Cloud-Modell aufgrund des damit einhergehenden Outsourcings der Bearbeitung und einer etwaigen Bekanntgabe (Transfer) von Personendaten ins Ausland weitere datenschutzrechtliche Fragen.

Schweizerisches Datenschutzrecht kann selbst dann zur Anwendung kommen, wenn eine Person mit Wohnsitz in der Schweiz eine Verletzung schweizerischen Datenschutzrechts durch einen Datenbearbeiter (Board Portal Provider) mit Sitz im Ausland geltend macht. Dies ergibt sich aus Art. 139 IPRG, welcher bestimmt, dass die eine Datenschutzverletzung geltend machende Person die Option hat, sich auf das *«Recht des Staates, in dem der Geschädigte seinen gewöhnlichen Aufenthalt hat»*, zu berufen, sofern der Schädiger (hier: Board Portal Provider/Gesellschaft) *«mit dem Eintritt des Erfolges in diesem Staat rechnen musste»*.[52]

1.2 Personendaten in Board Portalen

Gemäss Art. 3 lit. a DSG gelten alle Informationen als Personendaten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bei den Informationen kann es sich um objektive Tatsachen oder subjektive Werturteile handeln.[53] Abweichend von den meisten ausländischen Datenschutzgesetzen behandelt das DSG zumindest *de lege lata* auch die sich auf juristische Personen[54] beziehenden Informationen als Personendaten (siehe Art. 3 lit. b DSG).[55] Das schweizerische Datenschutzrecht schützt dementsprechend nicht nur die sich auf Angestellte, Beauftragte (wie VR-Mitglieder) oder sonstige Dritte (z.B. Bewerber) beziehenden Informationen, sondern auch Informationen betreffend Lieferanten, Kunden und Konkurrenzunternehmen einer Gesellschaft oder mögliche Übernahmekandidaten, die in ein Board Portal für den späteren Zugriff von und die Bearbeitung durch den VR hochgeladen werden. Der Begriff der «Personendaten» gemäss DSG ist somit weit gefasst. Dies, in Kombination mit einer eher extensiven Auslegungspraxis der Gerichte, führt dazu, dass häufiger, als gemeinhin angenommen wird, eine dem DSG unterstellte Datenbearbeitung vorliegt.[56]

1.3 Datenbearbeitungsgrundsätze

Das DSG beruht auf dem Prinzip, dass eine Datenbearbeitung keine Persönlichkeitsverletzung begründet, wenn der Datenbearbeiter (vorliegend: Gesellschaft

---

49 BSK DSG-Maurer-Lambrou/Kunz, Art. 2 N 19b f.; David Vasella, Social Media und Datenschutz, in: Staffelbach/Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015, 241 ff., Rn. 7.27.

50 Als Datenbearbeitung gilt gemäss Art. 3 lit. e DSG *«jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.»* Bereits das Speichern oder Löschen von Daten ist somit als Datenbearbeitung im Sinne des DSG zu qualifizieren.

51 Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1 (DSG) sowie Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993, SR 235.11 (VDSG).

52 Vasella (FN 49), Rn. 7.27 f.

53 Stefan Gerschwiler, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden (§ 3), 81/Rn. 3.28, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Zürich 2015, 73 ff.

54 Einschliesslich die nach Aussen rechtsfähigen Personenverbindungen wie Kollektiv- und Kommanditgesellschaften, BSK DSG-Blechta, Art. 3 N 21 f.; Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz, BBl 1988 II 413–534, 438.

55 Der Bundesrat hat am 1. April 2015 eine Revision des DSG gutgeheissen und das Eidgenössische Justiz- und Polizeidepartement beauftragt, unter Berücksichtigung der derzeit laufenden Datenschutzreformen in der EU und beim Europarat bis spätestens Ende August 2016 einen Vorentwurf für eine Revision des DSG zu unterbreiten. Obwohl der Entwurf noch nicht publiziert wurde, ist bereits durchgesickert, dass der Bundesrat auf den Schutz der Personendaten juristischer Personen verzichten möchte. Dies mit der Begründung, dass damit der grenzüberschreitende Datenverkehr verbessert werden könne, weil die Bekanntgabe von Daten juristischer Personen ins Ausland nicht mehr daran geknüpft sei, dass im Bestimmungsland ein angemessener Datenschutz gewährleistet wird (siehe Antwort des Bundesrates zur Motion Béglé (16.3379): «Förderung der Schweiz als universeller virtueller Datentresor»).

56 Gerschwiler (FN 53), 84/Rn. 3.28.

und Board Portal Provider) bestimmte Datenbearbeitungsgrundsätze einhält. Bei einer Datenbearbeitung auf Grundlage des DSG wird deshalb zutreffend von einer «Erlaubnis mit Verbotsvorbehalt» gesprochen.[57] Die Grundsätze der Datenbearbeitung sind in den Art. 4 (Grundsätze), Art. 5 (Richtigkeit) und Art. 7 DSG (Datensicherheit) geregelt. Werden Bearbeitungsgrundsätze nicht eingehalten, so liegt (vermutungsweise) eine Verletzung des Persönlichkeitsrechts der betroffenen Person vor (Art. 12 Abs. 2 lit. a DSG), die jedoch im Einzelfall aufgrund überwiegender (privater oder öffentlicher) Interessen, Einwilligung des Verletzten[58] oder durch Gesetz gerechtfertigt sein kann (Art. 13 DSG).[59]

Konkret hat die Gesellschaft bei der Bearbeitung von Personendaten in Board Portalen die folgenden Grundsätze zu beachten:

- **Grundsatz der Rechtmässigkeit** (Art. 4 Abs. 1 DSG): Personendaten müssen rechtmässig bearbeitet (dazu gehört auch das Beschaffen, siehe FN 38) werden. Eine unrechtmässige Datenbearbeitung liegt dann vor, wenn diese gegen eine in der Schweiz geltende, rechtlich verbindliche Norm verstösst, wie z.B. Art. 179 ff. StGB (Strafbare Handlung gegen den Geheim- oder Privatbereich), Art. 6 UWG (Verletzung von Fabrikations- und Geschäftsgeheimnissen) oder Art. 28 OR (Absichtliche Täuschung).
  Wenn Personendaten unrechtmässig beschafft worden sind, hat dies zur Folge, dass alle darauf folgenden Datenbearbeitungen unrechtmässig sind. Eine Weiterbearbeitung unrechtmässig beschaffter Personendaten bleibt somit grundsätzlich unrechtmässig.[60] Demzufolge würde die Gesellschaft, wenn sie von einem Dritten unrechtmässig beschaffte Personendaten in Sitzungsunterlagen integriert und diese über ein Board Portal zugänglich macht, gegen den Grundsatz der Rechtmässigkeit verstossen.
- **Grundsatz der Verhältnismässigkeit** (Art. 4 Abs. 2 DSG): Daraus erfolgt insbesondere, dass mit Personendaten möglichst sparsam umgegangen werden und mit anonymisierten Daten gearbeitet werden soll, wenn sich der Bearbeitungszweck damit angemessen erreichen lässt.[61]
- **Grundsatz der Erkennbarkeit der Beschaffung und des Bearbeitungszwecks** (Art. 4 Abs. 4 DSG): Sowohl die Beschaffung von Personendaten wie auch der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Darüber hinaus müssen auch weitere Umstände der Beschaffung, die für den Betroffenen relevant sind, wie insbesondere die Identität des Datenbearbeiters und, im Falle der Weitergabe von Personendaten an Dritte, die Kategorien möglicher Datenempfänger erkennbar sein.[62]
- **Grundsatz der Zweckbindung** (Art. 4 Abs. 3 DSG): Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Erkennbarkeit des Bearbeitungszwecks gemäss Art. 4 Abs. 4 DSG ist somit Grundlage für die Zweckbindung gemäss Art. 4 Abs. 3 DSG. Eine Zweckbindung setzt selbstredend voraus, dass bei der Beschaffung überhaupt ein Bearbeitungszweck besteht. Dadurch sind Datenbearbeitungen, die das Beschaffen von Personendaten «auf Vorrat» bedingen, wie z.B. das Data Warehousing[63] oder Data Mining[64], aus datenschutzrechtlicher Sicht problematisch.[65] Bei beiden Formen der Datenbearbeitung werden neue Informationen über Personen gewonnen (sog. Sekundärdaten) und einem bei der Datenerhebung nicht deklarierten Datenbearbeitungszweck zugeführt.[66]
- **Grundsatz von Treu und Glauben** (Art. 4 Abs. 2 DSG): Diese Bestimmung ist gewissermassen als Generalklausel konzipiert und auferlegt dem Datenbe-

---

57 Vasella (FN 49), Rn. 7.5.

58 Die Einwilligung muss nach angemessener Information und freiwillig erfolgen (Art. 4 Abs. 5 DSG, sog. «informed consent»). Wenn erst nach der Datenbeschaffung neue bzw. erstmalige Bearbeitungszwecke dazukommen, über die nicht schon bei der Datenbeschaffung informiert werden konnte, ist die Abgabe eines *informed consent* grundsätzlich ausgeschlossen. Die erst verspätet geschaffene Transparenz verletzt in diesem Fall den Erkennbarkeitsgrundsatz und den Grundsatz der Zweckbindung.

59 Wenn ein Rechtfertigungsgrund gegeben ist, fehlt es an der Widerrechtlichkeit der Persönlichkeitsverletzung, Rosenthal, Handkommentar DSG, Art. 4 N 3; Vasella (FN 49), Rn. 7.6.

60 Astrid Epiney/Daniela Nüesch, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden (§ 3), in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Zürich 2015, 88 ff., 89/Rn. 3.62 f.

61 Vasella (FN 49), Rn. 7.50.

62 Florent Thouvenin, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Big Data und Datenschutz – Gegenseitige Herausforderung, Publikation aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich Nr. 59, 61 ff., 63 f.; Vasella (FN 37), Rn. 7.106.

63 Beim Data Warehousing werden über einen längeren Zeitraum Daten aus unterschiedlichen Quellen gesammelt, nutzungsbezogen aufbereitet und zeit- sowie funktionsgerecht zur Verfügung gestellt, Epiney/Nüesch (FN 60), 94/Fn 116.

64 Beim Data Mining werden Daten miteinander kombiniert, um neue, noch nicht vorhandene Informationen zu gewinnen, Epiney/Nüesch (FN 60), 94/Fn 115.

65 Nur wenn im Einzelfall ein Rechtfertigungsgrund gegeben ist (z.B. gestützt auf Art. 13 Abs. 2 lit. c DSG), ist eine Datenbearbeitung mit Vorratsdatenspeicherung datenschutzrechtlich umsetzbar, Vasella (FN 37), Rn. 7.48.

66 Epiney/Nüesch (FN 49), 94/Rn. 3.86. Es ist durchaus denkbar, dass die aus dem Data Warehousing oder Data Mining generierten Personendaten dem VR als Entscheidungsgrundlage dienen. Wenn solche Personendaten in ein Board Portal geladen werden, liegt grundsätzlich ein Verstoss gegen den Grundsatz der Zweckbindung vor und der VR müsste die Betroffenen über die Modifikation des Datenbearbeitungszwecks informieren und ihre Einwilligung einholen; Epiney/Nüesch (FN 60), 93/Rn. 3.83.

arbeiter ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr.[67]

- **Keine Datenbearbeitung gegen den ausdrücklichen Willen der betroffenen Person**: Als weiteren Grundsatz kann das Verbot betrachtet werden, Personendaten nicht (ohne Rechtfertigungsgrund) gegen den ausdrücklichen Willen der betroffenen Person zu bearbeiten (Art. 12 Abs. 2 lit. b DSG).[68]
- Die **Grundsätze der Datenrichtigkeit** (Art. 5 DSG) und **Datensicherheit** (Art. 7 DSG[69]) sollen sicherstellen, dass die bearbeiteten Personendaten korrekt sind und nicht verfälscht werden können.[70]

Vorbehaltlich der Grundsätze der Datenrichtigkeit (Art. 5 DSG) und Datensicherheit (Art. 7 DSG) bereitet die Einhaltung der obigen Datenbearbeitungsgrundsätze dann keine oder zumindest keine grösseren Probleme, wenn die Gesellschaft Personendaten von Vertragspartnern auf der Grundlage schriftlicher Verträge (Arbeitsverträge, Aufträge, Disclosure Agreements für Due Diligences bei Akquisitionen, Verträge mit Lieferanten oder Kunden etc.) erhält. Dies trifft insbesondere auch auf die Personendaten der VR-Mitglieder selber zu, die in Board Portalen bearbeitet werden. Im Rahmen dieser Verträge kann durch Aufnahme entsprechender Bestimmungen (Datenschutzerklärungen) weitgehend gewährleistet werden, dass die Datenbearbeitung in Übereinstimmung mit den Datenbearbeitungsgrundsätzen erfolgt. Im Rahmen von Arbeitsverhältnissen wird der Arbeitgeber (Gesellschaft) in einem bestimmten Umfang direkt durch das Gesetz zur Bearbeitung von Daten über den Arbeitnehmer ermächtigt.[71] Die Gefahr von Datenschutzverletzungen besteht vorwiegend dann, wenn die Gesellschaft Personendaten ausserhalb vertraglicher Beziehungen – z.B. aufgrund eines Assessments von Konkurrenten,[72] Übernahmekandidaten oder Bewerbern[73] – oder auf Vorrat (Data Warehousing oder Data Mining) erhebt und weiter bearbeitet.

1.4 Allgemein zugängliche Personendaten

Die datenschutzrechtlichen Datenbearbeitungsgrundsätze müssen dann nicht befolgt werden, wenn die bearbeiteten Personendaten von der betroffenen Person allgemein zugänglich gemacht wurden und diese deren Bearbeitung nicht ausdrücklich untersagt haben (Art. 12 Abs. 3 DSG). Solche Daten können vom Datenbearbeiter (Gesellschaft bzw. Board Portal Provider) grundsätzlich frei und ohne Rechtfertigungsgrund bearbeitet, d.h. beispielsweise in ein Board Portal geladen, aufbereitet und für VR-Mitglieder zugänglich gemacht werden.[74]

Personendaten sind gemäss Art. 12 Abs. 3 DSG allgemein zugänglich, wenn die betroffene Person sie mit Wissen und Willen in einer Weise zugänglich macht, die es einer unbestimmten Zahl von Personen ermöglicht, die Personendaten ohne wesentliche Hindernisse in Erfahrung zu bringen.[75] Als allgemein zugänglich gemacht gelten etwa alle sich auf eine Person beziehenden Informationen (wie Personalien, Berufsbezeichnung, Adresse oder Telefonnummer) und Meinungen, welche die betroffene Person in einer öffentlichen Veranstaltung, in den Medien oder über frei zugängliche Webseiten bekannt gegeben hat.[76]

1.5 Auslagerung der Datenbearbeitung beim Cloud-Modell

Beim Umgang mit Personendaten können zwei Funktionen unterschieden werden: Der Controller ist diejenige Person, welche für die Datenbearbeitung verantwortlich ist und entsprechend über den Zweck und den Inhalt einer Datensammlung entscheidet (Art. 3 lit. i DSG). Der Processor ist die Person, die Daten gemäss Zweck und Inhalt bearbeitet. Handelt es sich beim Processor um eine andere Person als den Controller und fallen die beiden Funktionen somit auseinander, liegt eine sog. «Datenbearbeitung durch Dritte» gemäss Art. 10a DSG vor. Dies entspricht der Situation beim Cloud-Modell.[77] Die im Rahmen des Einsatzes eines Board Portals anfallenden Datenbearbeitungen sind an externe Provider ausgelagert. Die Anwendungen und Daten (inklusive Personendaten) befinden sich nicht mehr im eigenen Netzwerk der Gesellschaft, sondern in der Cloud des Providers. Der Zugang zu Daten, Services und Infrastruktur, die in der Cloud zur Verfügung gestellt werden, erfolgt meist über einen Webbrowser mittels Fernzugriff (remote access).[78]

---

67 Epiney/Nüesch (FN 60), 90/Rn. 3.71 f.

68 Vasella (FN 49), Rn. 7.7.

69 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Die vorzukehrenden Massnahmen sind in Art. 8 ff. DSV spezifiziert.

70 Näheres findet sich bei Epiney/Nüesch (FN 60), 98 f./Rn. 3.93 ff.

71 Gemäss Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.

72 Strategie und Initiativen der Konkurrenz, Positionierung der Konkurrenz etc.

73 Detailinformationen zu potentiellen externen Nachfolge-Kandidaten für Geschäftsleitung oder weitere Schlüsselpositionen.

74 Auch bei allgemein zugänglich gemachten Personendaten sind jedoch die öffentlich-rechtlichen Pflichten gemäss Art. 8 DSG (Auskunftsrecht), Art. 11a DSG (Anmeldepflicht), Art. 14 DSG (Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen) und Art. 6 Abs. 3 DSG (Informationspflicht bei der Bekanntgabe von Personendaten ins Ausland) einzuhalten; Vasella (FN 49), Rn. 7.21.

75 Rosenthal, Handkommentar DSG, Art. 12 Abs. 3 N 54.

76 BSK DSG-Rampini, Art. 12 N 3.

77 BSK DSG-Bühler/Rampini, Art. 10a N 22a. Beim In-House-Modell werden beide Funktionen von der Gesellschaft wahrgenommen.

78 Das am weitesten verbreitete Service-Modell für Cloud-Lösungen im Zusammenhang mit Board Portalen ist SaaS (software as a service). Bei SaaS ist der Cloud-Nutzer nur noch Konsument in der

Gemäss Art. 10a DSG Abs. 1 darf die Bearbeitung von Personendaten durch Vereinbarung oder Gesetz Dritten (hier: Board Portal Provider) übertragen werden, wenn (i) die Daten nur so bearbeitet werden, wie der Auftraggeber (hier: Gesellschaft) es selbst tun dürfte, und (ii) wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Der datenbearbeitende Dritte (Board Portal Provider) muss dabei verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Board Portal Provider beigezogen werden.[79] Im Weiteren muss sich die Gesellschaft vergewissern, dass der Board Portal Provider die Datensicherheit im Sinne von Art. 7 DSG gewährleistet (Art. 10a DSG Abs. 2). Dies bedeutet, dass die Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt sein müssen.

Der Umstand, dass ein Board Portal Provider eine etwaige verletzende Datenbearbeitung als Auftragsbearbeiter (Processor) vornimmt, befreit ihn grundsätzlich nicht von der Haftung für Datenschutzverletzungen. Sowohl die Gesellschaft als Auftraggebern wie auch der Board Portal Provider als Auftragsbearbeiter sind an die Grundsätze des Datenschutzrechts und insbesondere an die vorangehend erläuterten Datenbearbeitungsgrundsätze gebunden.[80] Wenn jedoch die Voraussetzungen gemäss Art. 10a DSG eingehalten werden, entsteht eine rechtliche Privilegierung der Gesellschaft (Auftraggebern) und des Board Portal Providers (Auftragnehmer), welche im Wesentlichen darin besteht, dass der Provider nicht als «Dritter» betrachtet wird und der Transfer von Personendaten von der Gesellschaft zum Provider entsprechend nicht als eine Datenbekanntgabe an Dritte gilt.[81] Der Transfer von Personendaten an den Provider im Rahmen von Art. 10a DSG setzt deshalb insbesondere nicht voraus, dass die damit einhergehende Datenbekanntgabe bei der Beschaffung der Personendaten der betroffenen Person erkennbar gemacht worden ist.[82] Vorausgesetzt ist freilich, dass die Gesellschaft mit dem Provider einen Datenbearbeitungsvertrag abschliesst, der die Anforderungen gemäss Art. 10a DSG umsetzt.

Von der Privilegierung gemäss Art. 10a DSG nicht erfasst sind die Pflichten, die gemäss Art. 6 DSG bei der grenzüberschreitenden Bekanntgabe von Personendaten zu beachten sind.[83] Im vorliegenden Zusammenhang sind diese Pflichten dann relevant, wenn eine schweizerische Gesellschaft im Rahmen eines Cloud-Modells einen Board Portal Provider mit Servern im Ausland beauftragt. Darauf ist nachfolgend genauer einzugehen.

2. Datenbekanntgabe ins Ausland

Eine Datenbekanntgabe[84] ins Ausland liegt dann vor, wenn Personendaten entweder aufgrund einer Bekanntgabe durch den Dateninhaber (vorliegend: Gesellschaft) oder aufgrund eines Abrufs durch den Datenempfänger im Ausland (vorliegend: Board Portal Provider) das Hoheitsgebiet der Schweiz verlassen.[85]

Keine Datenbekanntgabe ins Ausland liegt vor, wenn über ein mobiles Endgerät (Tablets, wie z.B. iPads) vom Ausland aus (etwa durch ein VR-Mitglied) auf Personendaten zugegriffen werden kann, die auf in der Schweiz stationierten Servern gespeichert sind. Dies gilt jedoch nur dann, wenn auf diese Weise entsprechende Informationen ohne Speicherung auf dem mobilen Gerät wahrgenommen werden können.[86] Darauf muss die Gesellschaft achten, wenn deren VR-Mitglieder von einem Land mit nicht angemessenem Datenschutz auf Board Portale zugreifen, die über Server in der Schweiz betrieben und zugänglich gemacht werden (dazu gleich im Anschluss). Die heutigen Board Portal Provider bieten in aller Regel entsprechende Funktionalitäten an, d.h. es kann gezielt gesteuert werden, ob die über ein Board Portal zugänglichen Dokumente nur angesehen oder auch heruntergeladen werden können. Sollte ein VR-Mitglied sein Endgerät im Ausland verlieren oder sollte es von ausländischen Behörden in Gewahrsam genommen werden, könnte zudem der Zugriff des entsprechenden VR-Mitglieds auf das Board Portal vollständig gesperrt werden.

Werden Personendaten ins Ausland bekannt gegeben, kann dies zu einer besonderen Gefährdung der davon

---

Cloud. Er bewirtschaftet nichts mehr selber, weder die Anwendungen noch die Daten. Ihm wird einzig in der Cloud eine Funktionalität zur Verfügung gestellt, um dort Daten bearbeiten zu können; EDÖB, Erläuterungen zu Cloud Computing, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de> (zuletzt besucht am 18. November 2016).

79 EDÖB, Erläuterungen zu Cloud Computing, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de> (zuletzt besucht am 18. November 2016).

80 Bühler/Rampini, BSK-DSG, Art. 10a DSG N 19; Rosenthal, Handkommentar DSG, Art. 10a N 86; Vasella (FN 49), Rn. 7.82.

81 In der Lehre wird teilweise von «Bekanntgabeprivileg» gesprochen, weil die Bekanntgabe von Personendaten vom Auftraggeber an den Auftragsdatenbearbeiter erleichtert wird; Bühler/Rampini, BSK-DSG, Art. 10a DSG N 18.

82 Rosenthal, Handkommentar DSG, Art. 10a N 24. Ebenso besteht keine Pflicht zur Registrierung der Datenbank gemäss Art. 11a DSG. Besonders schützenswerte Personendaten und Persönlichkeitsprofile dürfen zudem auch ohne Rechtfertigungsgrund ausgetauscht werden (Art. 12 Abs. 2 lit. c DSG); Vasella (FN 49), Rn. 7.82.

83 Vasella (FN 49), Rn. 7.82.

84 Gemäss Art. 3 lit. f DSG gilt «das Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen» als «Bekanntgabe».

85 EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG (Version vom April 2011), 4.

86 Nicolas Passadelis, Rechtsanwendung bei internationaler Datenbearbeitung durch Private (§ 6), 182/Rn. 6.41, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Zürich 2015, 167 ff.; BSK DSG-Maurer-Lambrou/Steiner, Art. 6 N 16.

betroffenen Personen führen. Art. 6 Abs. 1 DSG sieht deshalb vor, dass Personendaten nur dann ins Ausland bekannt gegeben werden dürfen, wenn dies die Persönlichkeit der betroffenen Person nicht schwerwiegend gefährdet. Eine solche Gefährdung besteht insbesondere dann, wenn im Ausland eine Gesetzgebung fehlt, die einen angemessenen gesetzlichen Schutz gewährleistet. Der EDÖB publiziert eine Liste jener Staaten, welche über einen angemessenen Datenschutz verfügen (Art. 7 DSV). Wenn ein Land nicht in dieser Liste aufgeführt ist, bedeutet dies nicht zwingend, dass kein angemessener Schutz besteht. Ein angemessener Schutz kann vielmehr auch über andere Vorkehrungen erzielt werden, wie insbesondere einen Staatsvertrag, der ein adäquates Schutzniveau implementiert.[87]

Zu den Staaten, die mangels angemessener Datenschutzgesetzgebung über einen Staatsvertrag einen angemessenen Datenschutz gewährleisten, gehören insbesondere die USA, welche mit der Schweiz das sog. «US-Swiss Safe Harbor Framework» abgeschlossen haben. Bei diesem Abkommen handelt es sich um ein bilaterales Datenschutzrahmenwerk, welches den Transfer von Personendaten aus der Schweiz in die USA regelt. Damit ein Daten empfangendes US-Unternehmen gestützt auf das Abkommen Personendaten aus der Schweiz empfangen und weiterbearbeiten darf, muss es sich verpflichten, gewisse Schweizer Datenschutzstandards einzuhalten und sich in die von der International Trade Administration (ITA) geführte Liste für Safe Harbor-zertifizierte US-Unternehmen eintragen lassen. Vor einer Datenübermittlung in die USA muss dann nur noch geprüft werden, ob das entsprechende US-Unternehmen aufgeführt ist.[88] Wenn dies zutrifft, dürfen Personendaten gestützt auf Art. 6 Abs. 1 DSG ohne weiteres in die USA transferiert werden. Im gegenteiligen Fall ist der Datentransfer nur zulässig, wenn eine der Massnahmen gemäss Art. 6 Abs. 2 DSG getroffen wird,[89] d.h. insbesondere die Einwilligung der betroffenen Personen eingeholt oder ein Datenübermittlungsvertrag mit dem ausländischen Datenempfänger geschlossen wird, der zur Einhaltung eines gewissen datenschutzrechtlichen Mindeststandards verpflichtet.

Die USA hat mit der EU ein paralleles, inhaltlich weitgehend übereinstimmendes Abkommen abgeschlossen (US-EU Safe Harbor Framework). Der von den zertifizierten US-Unternehmen zu gewährende Schutz hatte sich, anders als bei Datenübermittlungen gestützt auf das US-Swiss Safe Harbor Framework, nicht auf Personendaten juristischer Personen zu beziehen.[90] Aufgrund des nachfolgend erörterten Urteils des EuGH sind transatlantische Datentransfers sowohl gestützt auf das US-EU wie auch das US-Swiss Safe Harbor Framework jedoch nicht mehr möglich.

3. Safe Harbor-Urteil des EuGH

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, *Maximilian Schrems* vs. *Data Protection Commissioner,* die Entscheidung der Europäischen Kommission, wonach die USA gestützt auf das US-EU Safe Harbor Framework ein angemessenes Schutzniveau für übermittelte personenbezogene Daten gewährleisten, für ungültig erklärt. Der EuGH verwies dabei auf die Enthüllungen des ehemaligen Mitarbeiters der US National Security Agency, Edward Snowden, betreffend Massenüberwachungsmassnahmen der amerikanischen Geheimdienste.

Im Einzelnen hielt der EuGH fest, dass das US-EU Safe Harbor Framework insbesondere die folgenden Mängel aufweise:[91]

- Das Abkommen bindet ausschliesslich die US-Unternehmen, die sich den Regeln des Abkommens unterstellt haben, nicht aber die amerikanischen Behörden, die auf in den USA bearbeitete Personendaten zugreifen wollen.[92]
- Die Safe Harbor-zertifizierten US-Unternehmen bleiben inneramerikanischem Recht verpflichtet, wenn die datenschutzrechtlichen Vorgaben des Abkommens diesem widersprechen.[93]
- Die Kommission hat bei der Prüfung der Angemessenheit des Abkommens nicht geprüft, ob behördliche Zugriffe und Datenbearbeitungen nicht auf das absolut Notwendige zu beschränken sind.[94]
- Es besteht kein angemessener gerichtlicher Rechtschutz, d.h. es fehlt an einer effektiven Möglichkeit, Zugang zu den eigenen Personendaten zu erhalten

---

87 EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG (Version vom April 2011), 4.

88 EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG (Version vom April 2011), 6. Rund 4000 Unternehmen haben sich nach den Safe Harbor-Grundsätzen der Schweiz zertifizieren lassen, siehe US-Swiss Safe Harbor List, abrufbar unter <safeharbor.export.gov/swisslist.aspx> (zuletzt besucht am 18. November 2016).

89 Art. 6 Abs. 2 DSG regelt, unter welchen Umständen die ausnahmsweise Übermittlung von Personendaten trotz fehlendem angemessenem Datenschutzniveau im Empfängerland zulässig ist.

90 Mitteilung des EDÖB vom 1. Mai 2013, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00753/00970/index.html> (zuletzt besucht am 18. November 2016).

91 Iris Sidler/David Vasella, Aus Safe Harbor wird Privacy Shield: Folgen des Urteils des EuGH i.S. Schrems, sic! 2016, 185 ff., 187 f.

92 E. 82 des Urteils. Siehe auch die Ausführungen des EDÖB zur Gefahr ausländischer Behördenzugriffe beim Cloud Computing, EDÖB, Erläuterungen zu Cloud Computing, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de> (zuletzt besucht am 18. November 2016).

93 E. 85 ff. des Urteils.

94 E. 88 und E. 92 ff. des Urteils.

oder gegebenenfalls ihre Berichtigung oder Löschung zu erwirken.[95]

Aufgrund dieser Mängel schlussfolgerte der EuGH, dass das US-amerikanische Recht kein angemessenes Datenschutzniveau gewährleiste und der Angemessenheitsentscheid deshalb ungültig sei.[96] US-Unternehmen, die Personendaten aus der EU bearbeiten (Facebook, Google, Salesforce etc.), können sich seit Rechtskraft des Urteils nicht mehr darauf berufen, dass sie Safe Harbor-zertifiziert sind und dadurch ein angemessenes Datenschutzniveau gewährleisten. Gleiches gilt für europäische Unternehmen (z.B. Board Portal Provider), die Personendaten in den USA bearbeiten lassen.[97]

Die EU und die USA haben sich am 2. Februar 2016 auf die Grundzüge eines revidierten, an die Stelle des Safe Harbor-Framework tretenden Abkommens geeinigt, das sog. «EU-US Privacy Shield». Die Kommission hat dieses hinsichtlich des Datenschutzes für angemessen und mit dem Safe Harbor-Urteil des EuGH im Einklang stehend erklärt.[98] Entsprechend wurde das EU-US Privacy Shield auf den 1. August 2016 in Kraft gesetzt,[99] was von manchen Kreisen kritisiert wurde, wie insbesondere der Artikel-29 Datenschutzgruppe.[100] Die Artikel-29 Datenschutzgruppe vertritt die Auffassung, dass verschiedene europäische Datenschutzprinzipien nicht im Privacy Shield widerspiegelt sind (u.a. Löschungspflicht für nicht benötigte Personendaten, Anwendungsbereich des Grundsatzes der Zweckbindung nicht hinreichend klar definiert, Weitergabe durch Privacy Shield-zertifizierte Unternehmen an Dritte nicht hinreichend klar geregelt). Im Weiteren wurde kritisiert, die in Einzelfällen weiterhin zulässige Massenüberwachung von EU-Bürgern verstosse gegen europäisches Recht.

Erst kürzlich hat die Digital Rights Ireland Ltd. beim Europäischen Gerichtshof eine Nichtigkeitsklage gegen den Angemessenheitsbeschluss der Europäischen Kommission über das EU-US Privacy Shield vom 12. Juli 2016 eingereicht (Rechtssache T-670/16). Ob das EU-US Privacy Shield die vom EuGH aufgeworfenen Mängel des US-EU Safe Harbor Framework zu beseitigen vermag, wird somit aller Voraussicht nach vom EuGH abschliessend geklärt werden.

4. Auswirkungen des Safe Harbor-Urteils auf die Schweiz

Die Schweiz ist nicht EU-Mitglied und das Safe Harbor-Urteil somit an sich nicht verbindlich. Für die Schweiz ist es dennoch von grosser Bedeutung, dass sie in den Augen der EU weiterhin als Land mit angemessenem Datenschutz betrachtet wird. Ob aus Sicht der EU ein angemessener Schutz besteht, ist auch davon abhängig, wie die Schweiz Datentransfers in die USA regelt. Würde sie nicht mit der Beurteilung der EU gleichziehen, was als angemessener Datenschutz gilt, könnte dies dazu führen, dass Datenexporte aus der EU in die Schweiz nur noch unter erschwerten Bedingungen möglich sind, was letztlich den Wirtschaftsverkehr zur EU beeinträchtigt.[101] Aus diesen eher realpolitischen, daneben aber auch aus datenschutzrechtlichen und rechtsstaatlichen Überlegungen (Rechtsschutz, Schutz von Freiheits- bzw. Grundrechten)[102] wird in der Lehre und vom EDÖB[103] die Auffassung vertreten, die Bekanntgabe von Personendaten in die USA könne seit dem Urteil nicht mehr gestützt auf eine Safe Harbor-Zertifizierung erfolgen – dies obwohl das US-Swiss Safe Harbor Framework formell nach wie vor in Kraft ist.[104]

Aufgrund dieser Ausgangslage wird in der Praxis empfohlen, bei der Übermittlung von Personendaten von der Schweiz in die USA nicht mehr auf die Safe Harbor-Zertifizierung eines US-Unternehmens abzustellen,[105] sondern auf eine Einwilligung der betroffenen Personen (Art. 6 Abs. 2 lit. a DSG) oder Datenübermittlungsverträge (Art. 6 Abs. 2 lit. a DSG), insbesondere die EU-Standardvertragsklauseln,[106] die auch in der Schweiz an-

---

95 E. 89 und 95 des Urteils; E. 95: «Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.»

96 Sidler/Vasella (FN 91), 188.

97 Martin Steiger, Safe Harbor-Urteil: Wie weiter in der Schweiz?, Beitrag vom 7. Oktober 2015, abrufbar unter <https://steigerlegal.ch/2015/10/07/safe-harbor-urteil-schweiz/> (zuletzt besucht am 18. November 2016).

98 Sidler/Vasella (FN 91), 189 ff.

99 Siehe Medienmitteilung der Kommission vom 12. Juli 2016, abrufbar unter <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> (zuletzt besucht am 18. November 2016).

100 Diese hat Beratungsfunktion im Rahmen der EU-Datenschutzgesetzgebung. Die entsprechende Pressemitteilung der Artikel-29 Datenschutzgruppe (Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield) ist abrufbar unter <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf> (zuletzt besucht am 18. November 2016).

101 David Rosenthal/Barbara Kaiser, Datenschutz: Wie weiter mit Datenübermittlungen in die USA?, in: Jusletter 2. November 2015, 10 ff.

102 Näheres dazu bei Rosenthal/Kaiser (FN 101), 7 f. und 10 ff.; Sidler/Vasella (FN 91), 193 ff.

103 Stellungnahme des EDÖB vom 25. August 2016, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=de> (zuletzt besucht 18. November 2016).

104 Der EDÖB kann nur die Kündigung bzw. Suspendierung des Abkommens anregen, jedoch nicht inhaltlich darüber entscheiden, Rosenthal/Kaiser (FN 101), 11.

105 Sidler/Vasella (FN 91), 194; Rosenthal/Kaiser (FN 101), 13.

106 Der EDÖB veröffentlicht eine Liste der von ihm erstellten oder anerkannten Musterverträge oder Standardvertragsklauseln (Art. 6 Abs. 3, letzter Satz, VDSG). Derzeit sind dies die Folgenden: Die Standardvertragsklauseln der Europäischen Union, abrufbar unter <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>; der Mustervertrag des Europarats für die Sicherstellung eines angemessenen Datenschutzes im

erkannt sind und für den Datentransfer von der Schweiz in die USA verwendet werden können.

5. Bedeutung für die Wahl amerikanischer Board Portal Provider

Der Verlust der sehr einfach zu realisierenden und kostengünstigen Möglichkeit, den Datentransfer in die USA über eine Safe Harbor-Zertifizierung des Datenempfängers abzuwickeln, hat im Ergebnis zur Folge, dass ein Board Portal Provider mit Sitz in den USA in einen Datenübermittlungsvertrag eingebunden werden muss. Dies ist aber in der Praxis aufgrund der umfangreichen Pflichten, die in solchen Verträgen dem Datenempfänger auferlegt werden,[107] sowie des anwendbaren (nicht-amerikanischen) Rechts[108] und Gerichtsstands (ausserhalb der USA)[109] oftmals schwierig zu bewerkstelligen . Nach Auffassung des EDÖB müssten die Musterverträge und Standardvertragsklauseln bei Datentransfers in die USA aufgrund des Safe Harbor-Urteils sogar noch ergänzt werden. Einerseits mit einer Pflicht, die betroffenen Personen möglichst umfassend darüber zu informieren, dass ihre Daten in die USA übermittelt werden und dass die dortigen Behörden darauf zugreifen können. Andererseits mit einer Pflicht, betroffene Personen bei Geltendmachung ihrer Rechte in den USA im zumutbaren Rahmen zu unterstützen.[110] Der EDÖB muss vom Datenexporteur (vorliegend: die Gesellschaft) im Weiteren über die Nutzung der Musterverträge und Standardvertragsklauseln informiert werden (Art. 6 Abs. 3 DSG und Art. 6 DSV).

Erschwerend kommt hinzu, dass derzeit selbst die Zulässigkeit der EU-Standardvertragsklauseln in Frage gestellt ist. Dies, weil die irische Datenschutzbehörde (DPC) den EuGH ersucht hat, die Rechtmässigkeit der EU-Standardvertragsklauseln als Grundlage für den transatlantischen Datenaustausch zu beurteilen.[111] Weil die im Safe Harbor-Urteil des EuGH aufgezeigten Mängel – unverhältnismässige Zugriffe amerikanischer Behörden auf Personendaten, mangelnder Rechtsschutz gegen solche Zugriffe – auch durch den Abschluss von Datenübermittlungsverträgen nicht behoben werden, ist durchaus möglich, dass der EuGH den Datentransfer in die USA gestützt auf EU-Standardvertragsklauseln ebenfalls für unzulässig erklärt. Sollte dies so eintreffen, wäre im vorliegenden Zusammenhang eine Datenübermittlung an einen amerikanischen Board Portal Provider grundsätzlich nur noch gestützt auf eine Einwilligung der betroffenen Person zulässig, jedenfalls dann, wenn ein Provider das Board Portal über einen in den USA stationierten Server laufen lässt oder für die Disaster Recovery (Katastrophenwiederherstellung) auf Servern in den USA Backup-Kopien der Inhalte von Board Portalen erstellt.

Die Einholung der Einwilligung scheint jedoch in mehrfacher Hinsicht wenig praktikabel: Zum einen gilt sie nur «im Einzelfall» und muss deshalb einen konkreten Fall oder eine konkrete Situation betreffen.[112] Zum anderen dürfte die Einholung einer Einwilligung immer dann mit Schwierigkeiten behaftet sein (inklusive Verweigerung der Einwilligung), wenn die Gesellschaft Personendaten ausserhalb vertraglicher Beziehungen (z.B. aufgrund eines Assessments von Konkurrenten, Übernahmekandidaten oder Bewerbern) oder auf Vorrat (Data Warehousing oder Data Mining) erhebt. Die Einwilligung muss ferner stets freiwillig und nach angemessener Information erfolgen, was z.B. in Bezug auf Personendaten von Arbeitnehmern problematisch sein kann.[113] Schliesslich kann eine Einwilligung nach herrschender Lehre auch widerrufen werden, was ihre Praktikabilität für konstante Datentransfers einschränkt.[114]

Somit ist festzuhalten, dass die Wahl eines US-amerikanischen Board Portal Providers aus datenschutzrechtlicher Sicht problematisch ist, wenn der Provider Personendaten in den USA bearbeitet (Board Portal wird über Server in den USA betrieben) oder bearbeiten lässt (Backup). Beruht die Bekanntgabe in die USA nicht auf einem Datenübermittlungsvertrag oder einer Einwilligung, muss im Lichte des Safe Harbor-Urteils davon

---

Rahmen des grenzüberschreitenden Datenverkehrs, abrufbar unter <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/ModelContract_1992.pdf> und der Mustervertrag des EDÖB für das Outsourcing von Datenbearbeitungen ins Ausland, abrufbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html?lang=de> (alle Seiten zuletzt besucht am 18. November 2016).

107 Siehe z.B. Ziffer 5 des EU Standardvertrages für «Controller to Processor» Datenübertragungen.

108 Die vom EDÖB anerkannten Datenübermittlungsverträge (siehe diesbez. Fn 94) sehen als anwendbares Recht das Recht am Ort des Datenexporteurs vor.

109 Die vom EDÖB anerkannten Datenübermittlungsverträge (siehe diesbez. Fn 94) sehen als Gerichtsstand den Sitz des Datenexporteurs vor.

110 Stellungnahme des EDÖB vom 25. August 2016, abrufbar unter <www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=de> (zuletzt besucht am 18. November 2016).

111 Die entsprechende Mitteilung ist abrufbar unter <www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm> (zuletzt besucht am 18. November 2016).

112 Die betroffene Person kann nicht pauschal einwilligen und so die regelmässige und systematische Bekanntgabe ihrer Daten ins Ausland zu verschiedenen Zwecken und in verschiedenen Situationen ermöglichen. Bekanntgaben, welche unter gleichen Voraussetzungen (Empfänger, Zweck, allfällige Weiterleitung) erfolgen, können jedoch im Rahmen einer einzigen Einwilligung erfasst werden; EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG (Version vom April 2011), 8.

113 Roberta Papa/Thomas Pietruszak, Datenschutz im Personalwesen (§ 17), in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Zürich 2015, Rn. 17.7, 17.100 m.w.H. Art. 328 OR ermächtigt den Arbeitgeber zudem nicht zur Bekanntgabe von Personendaten in Länder mit nicht angemessenem Datenschutz.

114 Rosenthal/Kaiser (FN 101), 20.

ausgegangen werden, dass sie gegen schweizerisches Datenschutzrecht verstösst. Auf der anderen Seite kann die Befolgung dieser datenschutzrechtlichen Vorgaben mit praktischen Umsetzungsproblemen behaftet sein (Verweigerung/Widerruf der Einwilligung bzw. Verweigerung des Abschlusses eines Datenübermittlungsvertrags).

Schliesslich bleibt abzuwarten, ob die Zusagen der USA gemäss EU-US Privacy Shield auch an die Adresse der Schweiz erfolgen und die Schweiz damit erneut ein paralleles Datenschutzabkommen mit den USA abschliessen kann (d.h. ein US-Swiss Privacy Shield).[115] Über entsprechende Verhandlungen ist derzeit nichts bekannt. Eine etwaige Gutheissung der Nichtigkeitsklage gegen den Angemessenheitsbeschluss der Europäischen Kommission betreffend das EU-US Privacy Shield (siehe dazu Ziff. 3 vorangehend) würde den Abschluss eines US-Swiss Privacy Shield sicherlich erschweren.

6. Wahl eines Board Portal Provider in der EU

Aufgrund des Umstands, dass gemäss der EU-Richtlinie[116] nur Personendaten von natürlichen Personen vom Datenschutz erfasst werden, besteht in den meisten EU-Staaten für Personendaten juristischer Personen kein angemessener Schutz.[117] Wenn somit eine Gesellschaft mit Sitz in der Schweiz einen Board Portal Provider beauftragt, der über Server in der EU verfügt, geht dies mit der Bekanntgabe von Personendaten in ein (EU-) Land mit nicht angemessenem Schutz für Personendaten juristischer Personen einher. Zumindest bei strenger Auslegung des Gesetzes bedarf diese Bekanntgabe von Personendaten juristischer Personen in das entsprechende EU-Land deshalb eines besonderen Rechtfertigungsgrundes gemäss Art. 6 Abs. 2 DSG (z.B. eines Datenübermittlungsvertrages, der zwischen der Gesellschaft und dem Board Portal Provider abgeschlossen wird).[118]

V. Zugriff von Behörden auf Informationen in Board Portalen

Eine wichtige Frage im Zusammenhang mit Board Portalen ist, ob und unter welchen Voraussetzungen staatliche Behörden im Rahmen eines Verfahrens auf die Informationen in den Board Portalen zugreifen können. Neue Überwachungsmöglichkeiten stellen potentiell die Vertraulichkeit in Frage. Dies gilt insbesondere hinsichtlich US-Behörden. Wie spätestens seit den Enthüllungen von Edward Snowden bekannt ist, überwachen diese den Datentransfer im grossen Stil. Im Weiteren haben US-Behörden in vergangenen Jahren immer häufiger (ausländische) Unternehmen ins Visier genommen und mit sehr hohen Bussen oder sonstigen Auflagen belastet. Schlussendlich ist die USA als Mekka der Hightech-Branche und des Board Portal-Marktes auch Sitz wichtiger Board Portal Provider. Es soll daher die Rechtslage in der Schweiz und in den USA näher erörtert werden.

1. Zugriff von Schweizer Behörden auf Board Portale in der Schweiz

Ob und unter welchen Voraussetzungen ein Zugriff der Behörden auf die Daten erfolgen kann, hängt von dem untersuchten Sachverhalt und der untersuchenden Behörde ab. Den umfangreichsten Zugriff auf Daten haben Strafverfolgungsbehörden und der Nachrichtendienst. Es bestehen im Weiteren auch gewisse Zugriffsrechte von Verwaltungsbehörden.

1.1 Grundrechtsschutz

In der Schweiz bestehen Grundrechte, welche zu beachten sind, wenn Behörden auf Daten zugreifen möchten. Gemäss Art. 13 Abs. 1 BV hat jede Person Anspruch auf Achtung ihrer Privatsphäre, ihrer Wohnung sowie des Brief-, Post- und Fernmeldeverkehrs. Gleichartige Garantien enthalten Art. 8 Ziff. 1 EMRK und Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR).[119] Relevant ist ferner auch die Wirtschaftsfreiheit (Art. 27 BV) sowie bei einer Beschlagnahme die Eigentumsgarantie (Art. 26 BV).

Alle Zwangsmassnahmen müssen daher den Voraussetzungen für Einschränkungen der Grundrechte genügen. Erforderlich ist zunächst eine genügende gesetzliche Grundlage. Ferner muss der Eingriff im öffentlichen Interesse liegen, verhältnismässig sein und der Kerngehalt der Verfassungsgarantien muss gewahrt bleiben (Art. 36 BV, Art. 8 Ziff. 2 EMRK, Art. 17 Ziff. 2 IPBPR).

---

115 In der Lehre wird damit gerechnet, siehe Rosenthal/Kaiser (FN 101), 22; Sidler/Vasella (FN 91), 195.

116 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

117 Ähnliche Regelungen sehen nur die Datenschutzgesetze des Fürstentums Liechtenstein und, mit Einschränkungen, Dänemarks vor; Vasella (FN 49), Rn. 7.12.

118 EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG (Version vom April 2011), 6; Gianni Fröhlich-Bleuler, Softwareverträge, 2. A., Bern 2014, 739 f./ Rn. 2855; a.M. Rosenthal, der die Auffassung vertritt, dass Personendaten von juristischen Personen frei exportiert werden dürfen, sofern sich im Einzelfall nicht ergibt, dass eine schwerwiegende Gefährdung der Persönlichkeit der juristischen Person besteht (bspw. weil sensitive Kundendaten ins Ausland exportiert werden), Rosenthal, Handkommentar DSG, Art. 6 N 34.

119 Siehe hierzu etwa BGE 140 IV 184; Andreas Donatsch/Albert Schmid, Der Zugriff auf E-Mails im Strafverfahren – Überwachung [BÜPF] oder Beschlagnahme?, in: Schwarzenegger und andere (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, 152 f.

1.2 Nachrichtendienstgesetz

Am 25. September 2016 wurde das Nachrichtendienstgesetz (NDG) vom Volk angenommen.[120] Dieses erweitert die möglichen Überwachungsmassnahmen des Schweizer Nachrichtendiensts. Es erlaubt unter anderem die Überwachung des Internetverkehrs und das Eindringen in Computersysteme und Computernetzwerke. Eingeführt wird u.a. auch die Möglichkeit zur Kabelaufklärung. Hierbei wird der Internetverkehr nach Suchbegriffen durchforstet.[121] Die Überwachungsmassnahmen im NDG finden grundsätzlich geheim statt, ohne die betroffenen Personen zu informieren.[122]

Das NDG sieht aber auch erhebliche Einschränkungen und Schutzmassnahmen vor. Die Massnahmen dürfen nur hinsichtlich schwerwiegender Bedrohungen der inneren oder äusseren Sicherheit (etwa im Zusammenhang mit Terrorismus, Massenvernichtungswaffen oder Cyberattacken auf kritische Infrastrukturen) ergriffen werden. Es besteht zudem eine relativ strenge Verhältnismässigkeitsprüfung.[123] Die Massnahmen bedürfen des Weiteren immer einer gerichtlichen Genehmigung.[124] Werden die Voraussetzungen für die Überwachungsmassnahmen beachtet, sollten prinzipiell die Unterlagen im Board Portal bzw. die Tätigkeit eines Unternehmens nicht in den Fokus des NDG geraten. Die gerichtliche Genehmigungspflicht sollte zudem sicherstellen, dass diese materiellen Voraussetzungen auch durchgesetzt werden. Am ehesten denkbar wäre, dass Informationen aus Board Portalen per Zufall Gegenstand einer Überwachung sind. Hierbei fragt sich, ob mögliche Zufallsfunde, welche hinsichtlich anderer Regelungsbereiche relevant sind, an die entsprechenden Behörden weitergegeben werden. Die Gefahr diesbezüglich scheint für Unternehmen, die Board Portale nutzen, eher gering. Es werden nur dann personenbezogene Daten an inländische Behörden weitergeleitet, wenn dies zur Wahrung der inneren und äusseren Sicherheit notwendig ist (Art. 60 Abs. 1 NDG). Dienen Erkenntnisse anderen Behörden zur Strafverfolgung, zur Verhinderung von schweren Straftaten oder zur Aufrechterhaltung der öffentlichen Ordnung, so stellt der NDB (Nachrichtendienst des Bundes) ihnen diese unter Wahrung des Quellenschutzes zur Verfügung (Art. 60 Abs. 2 NDG). Daten aus einer genehmigungspflichtigen Beschaffungsmassnahme werden einer Strafverfolgungsbehörde nur dann weitergeleitet, wenn konkrete Anhaltspunkte für eine Straftat bestehen und die Strafverfolgungsbehörde zur Verfolgung der betreffenden Straftat eine vergleichbare strafprozessuale Massnahme (siehe hierzu nachfolgend Ziffer 1.3a) anordnen dürfte.

1.3 Zugriffsrechte im Rahmen der StPO

Es bestehen zwei Möglichkeiten, wie Strafverfolgungsbehörden Informationen auf Board Portalen erlangen können. Es ist hierbei zu unterscheiden zwischen

- einer **heimlichen Überwachung** des Datenverkehrs, von welcher die betroffene Person nichts weiss (siehe a); und
- der Untersuchung und **Beschlagnahme** der Daten(träger), welche den Betroffenen aber mitgeteilt werden muss (siehe b).[125]

Die heimliche Überwachung ist in Art. 269 ff. StPO sowie dem BüPF[126] und dem VüPF[127] geregelt. Die gesetzlichen Bestimmungen zur Untersuchung und Beschlagnahme der Informationen unter Mitteilung an die Betroffenen finden sich schwergewichtig in Art. 246 ff. StPO sowie Art. 263 ff. StPO.

a. Überwachung

Hinsichtlich der Überwachung kann zwischen der Überwachung in Echtzeit und der rückwirkenden Überwachung unterschieden werden. Die Echtzeit-Überwachung ist das Abfangen in Echtzeit und die simultane, leicht verzögerte oder periodische Übertragung der Fernmeldeverkehrsdaten, inklusive Nutzinformationen, durch die Anbieterinnen von Post- oder Fernmeldediensten.[128] Die rückwirkende Überwachung beinhaltet die Herausgabe der Verkehrs- und Rechnungsdaten (d.h. der Randdaten) der zurückliegenden sechs Monate durch die Anbieterinnen von Post- oder Fernmeldediensten.[129] Die rückwirkende Überwachung betrifft nur die Randdaten, aber nicht den Inhalt des Fernmeldeverkehrs.[130] Es wird hier im Wesentlichen darüber Auskunft gegeben, wann und zwischen wem Verbindungen stattgefunden haben.[131]

Ein neuerer Bundesgerichtsentscheid befasst sich mit der Unterscheidung zwischen diesen Formen der Überwachung und der Beschlagnahme. Danach gelten hinsichtlich der Informationen des Fernmeldeverkehrs, die noch nicht im Herrschaftsbereich der betroffenen Person

---

120 Das NDG tritt voraussichtlich im September 2017 in Kraft.

121 Siehe Art. 39 ff. NDG zu den Voraussetzungen und den Einschränkungen hinsichtlich der Kabelaufklärung.

122 Siehe aber Art. 33 NDG zur Mitteilungspflicht nach Beendigung.

123 Die Bedrohung muss die Massnahme rechtfertigen und andere Abklärungen hätten erfolglos oder aussichtslos oder unverhältnismässig erschwert sein müssen, Art. 27 NDG.

124 Bei besonderer Dringlichkeit kann diese bei gewissen Massnahmen auch erst im Nachhinein erteilt werden (siehe Art. 31 NDG).

125 Vgl. BSK StPO-Jean-Richard-Dit-Bressel, Art. 269 N 21 ff.; BSK StPO-Thormann/Brechbühl, Art. 246 N 5.

126 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs.

127 Verordnung über die Überwachung des Post- und Fernmeldeverkehrs.

128 VüPF Anhang Ziff. 3.

129 VüPF Anhang Ziff. 4; BGE 140 IV 183.

130 BGE 139 IV 99; BSK StPO-Jean-Richard-Dit-Bressel, Art. 269 N 5 m.w.H.; Donatsch/Schmid (FN 119), 154.

131 BGE 140 IV 186.

liegen, die Voraussetzungen der Überwachung. Dies ist etwa der Fall bei E-Mails, bevor die betroffene Person ihr Konto abruft, d.h. eine Verbindung mit dem Server des Providers herstellt und das E-Mail für sie sichtbar macht. Bereits abgerufene Informationen aus dem Fernmeldeverkehr (z.B. abgerufene E-Mails) können hingegen – soweit sie dort noch vorhanden sind – auf dem Server des Providers beschlagnahmt werden. Hier gelten die Voraussetzungen der Beschlagnahme.[132]

Am höchsten sind die Anforderungen bei der Überwachung des Fernmeldeverkehrs in Echtzeit. Diese kann nach Art. 269 StPO angeordnet werden, wenn:

1. dringender Verdacht besteht, dass eine vom StPO genannte Straftat begangen wurde (Katalogtat);
2. die Schwere der Straftat die Überwachung rechtfertigt; und
3. die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden.

Bei den Katalogtaten handelt es sich um Delikte des klassischen Strafrechts, die kaum je in der Funktion eines VRs ausgeführt werden. Mögliche relevante Delikte sind insbesondere das Ausnützen von Insiderinformationen, Bestechung (v.a. von fremden Amtsträgern) und qualifizierte Formen der Geldwäscherei. Ausnahmsweise kommen auch Vermögensdelikte (z.B. Betrug, Veruntreuung, qualifizierte Formen ungetreuer Geschäftsführung) in Betracht. Die Voraussetzungen für eine rückwirkende Auskunft über die Randdaten sind niedriger.[133] Insbesondere bedarf es keiner Katalogtat (Art. 273 StPO). Beide Formen der Überwachung werden von der Staatsanwaltschaft angeordnet, müssen aber innert 24 Stunden dem Zwangsmassnahmengericht zur Genehmigung eingereicht werden (Art. 272 sowie Art. 273 Abs. 2 i.V.m. Art. 274 Abs. 1 StPO).

Zu beachten ist ferner, dass im aktuell gültigen BüPF die Überwachungspflichten nur Anwendung auf die staatlich konzessionierten oder meldepflichtigen Post- und Fernmeldedienste-Anbieterinnen sowie «Internet-Anbieterinnen» finden (Art. 1 Abs. 2 BüPF). Hierunter fallen nur Zugangs-Anbieterinnen (Access Provider), nicht aber reine Dienste-Anbieter (Service Provider).[134] Board Portale sind i.d.R. wohl keine Access Provider. Die Strafverfolgungsbehörden können daher unter derzeitigem Recht i.d.R. nicht auf den Inhalt in den Board Portalen zugreifen.[135]

Mit der Revision des BüPF[136] werden künftig neu auch Anbieterinnen abgeleiteter Kommunikationsdienste erfasst.[137] Hierunter fallen i.d.R. auch Board Portal Provider. Anbieterinnen abgeleiteter Kommunikationsdienste haben aber im neuen BüPF geringere Pflichten. Insbesondere müssen sie in der Regel die Überwachung nur dulden, aber es besteht keine aktive Überwachungspflicht.[138]

b. Beschlagnahme

Andere Voraussetzungen gelten hinsichtlich der offenen Durchsuchung und Beschlagnahme der Informationen bzw. der Datenträger. Die Vorrausetzungen sind hier bei Board Portalen im Wesentlichen die gleichen wie bei Unterlagen in Papierform. Es besteht aber faktisch hinsichtlich Board Portalen eine gewisse Erleichterung für die Behörden, da bei den Servern zentral auf die Informationen zugegriffen werden kann.

Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen dürfen durchsucht werden, wenn zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen (Art. 246 StPO). Gegenstände können unter anderem beschlagnahmt werden, wenn diese als Beweismittel gebraucht werden (Art. 263 Abs. 1 lit. a StPO).[139] Gewisse Informationen dürfen nicht beschlagnahmt werden (Art. 264 StPO).[140] Dies sind insbesondere die Unterlagen aus dem Verkehr der Beschuldigten mit ihrer Verteidigung oder mit Personen, denen ein Zeugnisverweigerungsrecht nach Art. 170–173 StPO zusteht (insbesondere aufgrund eines Berufs- oder Amtsgeheimnisses). Auch ausgeschlossen sind Unterlagen aus dem Verkehr einer anderen Person mit einem Rechtsanwalt,[141] der zur Vertretung vor Schweizer Gerichten zugelassen ist.[142] Dies

---

132 BGE 140 IV 187.

133 Diese Form der Überwachung scheint jedoch weniger relevant für Board Portale, da sie nicht den eigentlichen Inhalt des Fernmeldeverkehrs erfasst.

134 Vgl. Art. 1 Abs. 2 lit. e VÜPF und Ziff. 1 im Anhang zum VÜPF (Begriffe und Abkürzungen) sowie Samuel Klaus/Roland Mathys, «The Best of BÜPF» – Was ändert sich mit der Revision?, Rz. 5, in: Jusletter IT 22. September 2016.

135 Je nach technischer Ausgestaltung könnte man theoretisch auch über Access-Provider auf den Inhalt zugreifen. Board Portale sind i.d.R. aber technisch so organisiert, dass dies nicht möglich ist.

136 Die Referendumsfrist zum revidierten BüPF ist am 7. Juli 2016 unbenutzt abgelaufen. Das revidierte BÜPF dürfte gemäss Auskunft der Behörden per 2018 in Kraft treten. Zu den Änderungen in der Revision: Botschaft zum BÜPF vom 27. Februar 2013, BBl 2013 2683 ff.; Klaus/Mathys (FN 134), Rz. 1 ff.

137 Ausführlich Botschaft zum BÜPF (FN 136), 2707 ff.; Klaus/Mathys (FN 134), Rz. 20 ff.

138 Art. 27 Abs. 1 nBÜPF; Klaus/Mathys (FN 134), Rz. 22 ff.

139 Die weiteren Gründe für eine Beschlagnahme (z.B. Sicherstellen von Verfahrenskosten oder Geldstrafen, Einziehung) werden bei Board Portalen kaum je relevant sein. Ausführlich zu den Voraussetzungen der Beschlagnahme BSK StPO-Bommer/Goldschmid, Art. 263 N 9 ff.

140 Ausführlich hierzu und zu gewissen Gegenausnahmen BSK StPO-Bommer/Goldschmid, Art. 264 N 2 ff.

141 Voraussetzung hierfür ist, dass der Anwalt nicht selber beschuldigt ist.

142 Siehe hierzu Peter Burckhardt/Roland M. Ryser, Die erweiterten Beschlagnahmeverbote zum Schutz des Anwaltsgeheimnisses insbesondere im neuen Strafverfahren, AJP 2013, 159 ff.

kann insbesondere relevant sein, wenn sich eine Korrespondenz des VRs mit einem Anwalt auf dem Board Portal befindet, der VR aber nicht selber beschuldigt ist. Ein weiteres Beispiel wäre etwa ein Untersuchungsbericht, den eine schweizerische Anwaltskanzlei für das Unternehmen erstellt hat, wobei aber nicht das Unternehmen oder gar der VR, sondern ein Angestellter Beschuldigter ist.[143] Erwähnenswert ist hierbei, dass ausländische Kanzleien dieses Privileg nicht geniessen.[144] Das Anwaltsprivileg gilt ferner auch nicht, wenn ein VR-Mitglied zwar Anwalt ist, aber die Korrespondenz im Rahmen seiner Funktion als VR-Mitglied und nicht als Anwalt stattgefunden hat.[145] Darüber hinaus sind wie bei jeder Zwangsmassnahme die Grundsätze des Verhältnismässigkeitsgebots zu beachten.[146]

Es besteht ein besonderes Verfahren hinsichtlich der Durchsuchung von Informationen.[147] Der Inhaber kann sich hierzu vorgängig äussern und die Siegelung verlangen, worauf die Strafverfolgungsbehörde innert 20 Tagen ein Entsiegelungsgesuch stellen muss. Liegt ein Entsiegelungsgesuch vor, muss ein Gericht innerhalb eines Monats endgültig hierüber entscheiden.[148] Ziel des Entsiegelungsverfahrens ist es zu verhindern, dass die Strafverfolgungsbehörde Kenntnis von Informationen erlangt, obwohl die diesbezüglichen Voraussetzungen nicht erfüllt sind.[149]

1.4 Zugriff auf Informationen im Bereich des Verwaltungsrechts

Im Bereich des Verwaltungsrechts hängen die Zugriffsmöglichkeiten der Behörden von der jeweilig anwendbaren Rechtsgrundlage ab. Für Unternehmen sind in der Praxis insbesondere Massnahmen von Aufsichtsbehörden wie etwa der FINMA, Swissmedic oder den Wettbewerbsbehörden relevant.[150]

Eine Echtzeit-Überwachung des Fernmeldeverkehrs, wie sie oben in Ziffer 1.3a beschrieben wurde, kommt hier grundsätzlich nicht zur Anwendung. Diese ist nur für die in Art. 269 StPO genannten Katalogtaten zulässig.[151]

I.d.R. haben beaufsichtigte Unternehmen eine Auskunfts- und Herausgabepflicht. So eine Pflicht besteht z.B. im Bereich des Finanzmarktrechts unter Art. 29 FINMAG. Diese Pflichten gelten normalerweise aber nicht für Dritte, wie etwa den Board Portal Provider. Da die Informationen auf dem Board Portal aber noch im Herrschaftsbereich des beaufsichtigten Unternehmens sind, kann das Unternehmen i.d.R. verpflichtet werden, die Daten falls nötig selber herauszugeben.[152] Darüber hinaus sehen gewisse Spezialgesetze weitergehende Zugriffsrechte vor. Besonders stark ausgeprägt ist dies im Kartellgesetz.[153] Die Wettbewerbsbehörden können gemäss Art. 42 Abs. 2 KG i.V.m. Art. 45–50 VStrR Hausdurchsuchungen anordnen und Beweisgegenstände sicherstellen. Als Beweisgegenstände kommen hierbei auch Datenträger in Betracht, auf denen elektronische Daten gespeichert sind.[154] Die Voraussetzungen, um Informationen zu beschlagnahmen, sind vergleichbar wie im Strafverfahren (siehe Ziffer 1.3b). Es besteht ebenfalls ein Äusserungsrecht des Inhabers und ein Siegelungsverfahren.[155]

Abgesehen von den Rechtsgrundlagen in Spezialgesetzen sieht auch das VwVG hinsichtlich Verwaltungsverfahren vor Bundesbehörden[156] gewisse Zugriffsrechte vor. Wenn das Unternehmen Gegenstand eines formellen Verfahrens ist, besteht gemäss Art. 13 Abs. 1 VwVG eine Pflicht, an der Feststellung des Sachverhalts mitzuwirken, sofern das Unternehmen das Verfahren durch seine Begehren eingeleitet hat oder darin selbständige Begehren stellt.[157] Drittpersonen, wie Board Portale, können nach Art. 14 Abs. 1 und Art. 17 VwVG von gewissen Bundesbehörden (z.B. FINMA, EJPD) zur Vorlage von Informationen verpflichtet werden, wenn sich ein Sachverhalt auf andere Weise nicht hinreichend abklären lässt.[158]

Weitgehende Zugriffsrechte können sich ferner hinsichtlich von Straftaten aus Spezialgesetzen ergeben. Hinsichtlich Straftaten, für deren Verfolgung Bundesbehörden zuständig sind, gilt das VStrR[159] (vgl. zu den Zugriffsrechten, die hierunter möglich sind, die obigen

---

143 Burckhardt/Ryser (FN 142), 164 f.
144 Burckhardt/Ryser (FN 142), 165.
145 Vgl. BSK StPO-Bommer/Goldschmid, Art. 264 StPO N 26; Burckhardt/Ryser (FN 142), 161.
146 Siehe hierzu BSK StPO-Bommer/Goldschmid, Art. 263 N 23.
147 Siehe Art. 247 ff. StPO. Ausführlich hierzu BSK StPO-Thormann/Brechbühl, Art. 246.
148 Siehe zum Entsiegelungsverfahren Thomas Müller/Stephan Gäumann, Siegelung nach Schweizerischer StPO, Anwaltsrevue 2012, 290 ff.; BSK StPO-Thormann/Brechbühl, Art. 248 N 1 ff.
149 BSK StPO-Thormann/Brechbühl, Art. 248 N 40.
150 Von Bedeutung sind ferner insbesondere auch die Steuerbehörden.
151 BSK KG-Bangarter, Art. 42 N 47.
152 Dies ist etwa der Fall unter Art. 29 FINMAG; BSK FINMAG-Truffer, Art. 29 N 14 m.w.H.
153 In anderen Bereichen sind die Zugriffsrechte mittels Zwangsmassnahmen i.d.R. deutlich weniger weitgehend als im Kartellrecht.
154 BGE 108 V 76; BSK KG-Bangarter, Art. 42 N 70 m.w.H.
155 Es ist umstritten, ob auf Daten zugegriffen werden kann, die sich ausserhalb des räumlichen Durchsuchungsbereichs befinden. Dies ist etwa der Fall, wenn sich die Daten auf dem Server eines Serviceproviders, wie beispielsweise Board Portalen, befinden; BSK KG-Bangarter, Art. 42 N 131. Das Bundesgericht hat dies für die Beschlagnahme im Rahmen der StPO bejaht, BGE 140 IV 187. Es ist daher davon auszugehen, dass gleiches für die Beschlagnahme im Rahmen des KG gilt.
156 Auf kantonaler Stufe gelten die kantonalen Verfahrensbestimmungen.
157 Siehe ferner auch Art. 18 VwVG i.V.m. Art. 50 BZP.
158 Siehe ferner auch Art. 18 VwVG i.V.m. Art. 51 BZP.
159 Teilweise kommt auch die StPO zur Anwendung. Für eine Übersicht über den Anwendungsbereich des VStR siehe Andreas Eicker/Friedrich Frank/Jonas Aschermann, Verwaltungsstrafrecht und Verwaltungsstrafverfahrensrecht, Bern 2012, 21 ff.

Ausführungen zum Kartellgesetz).[160] Sind die normalen Strafverfolgungsbehörden für die Verfolgung zuständig, gelten die Verfahrensvorschriften in der StPO (siehe Ziffer 1.3).[161]

2. Zugriff von US-Behörden auf Board Portale in den USA

2.1 Grundrechtsschutz

Die US-amerikanische Verfassung statuiert nicht ein explizites Recht auf Datenschutz oder Schutz der Persönlichkeit. Der Schutz vor staatlichen Zugriffen in einen grundsätzlich geschützten, persönlichen Bereich ist aber im vierten Verfassungszusatz verankert, welcher den Schutz der Person und der Wohnung vor Durchsuchungen gewährleistet.[162] Der US Supreme Court hat jedoch bis anhin kein allgemeines Recht auf informationelle Selbstbestimmung, Schutz der Persönlichkeit oder Datenschutz anerkannt.[163] Unbestritten ist, dass der vierte Verfassungszusatz einen gewissen Schutz vor unverhältnismässigen elektronischen Überwachungsmassnahmen und Beschlagnahmungen bietet.[164]

Bezugnehmend auf die Grenzen der Geltung des Schutzes von Personendaten gemäss US-EU Safe Harbor-Abkommen aufgrund des generellen Vorrangs US-amerikanischer Gesetze und damit verbundener Zugriffsmöglichkeiten von US-Behörden, hielt der EuGH Folgendes fest: *«Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen […].»* Insbesondere würde eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta der Grundrechte der Europäischen Union garantierten Grundrechts auf Achtung des Privatlebens.[165] Ob dies in Bezug auf die Zugriffsrechte US-amerikanischer Behörden zutreffend ist, scheint der EuGH freilich nicht geprüft zu haben. Er monierte lediglich, dass die Kommission bei ihrem Angemessenheitsentscheid nicht geprüft habe, ob US-amerikanische Rechtsvorschriften Grundrechtseingriffe angemessen begrenzen. Das US-EU Safe Harbor-Abkommen selber würde US-amerikanischen Behörden keine entsprechenden Grenzen auferlegen.[166]

2.2 Nachrichtendienste

Die nicht an einen konkreten Tatverdacht geknüpften Überwachungsmassnahmen beruhen in erster Linie auf dem USA Patriot Act[167] und dem Foreign Intelligence Surveillance Act (FISA).[168]

Eine Überwachung gemäss Section 215 des USA Patriot Act muss von einer gerichtlichen Behörde genehmigt werden und darf nicht ausschliesslich auf die Aktivitäten einer amerikanischen Person abzielen, welche durch den ersten Verfassungszusatz (freedom of speech) geschützt ist. Gemäss der im USA Patriot Act verankerten business records-Regel sind Geheimdienste gestützt auf einen Durchsuchungsbefehl ferner berechtigt, die Herausgabe von Gegenständen («any tangible thing») zu verlangen,[169] wenn dies für eine internationale Anti-Terror-Ermittlung «relevant» ist. Die bisherige Praxis zeigt, dass der Begriff «relevant» extensiv ausgelegt wird. Der richterliche Entscheid und die Ausführung der Überwachung bzw. Beschlagnahme sind geheim. Der Generalstaatsanwalt hat lediglich die zwei Geheimdienstkomitees des Senats und Repräsentantenhauses halbjährlich über alle erteilten Überwachungsverfügungen zu infor-

---

160 Ausführlich hierzu Eicker/Frank/Aschermann (FN 158), 187 ff.

161 Hinsichtlich Straftatbestände aus kantonalem Recht haben die Kantone theoretisch die Möglichkeit, kantonale Verfahrensvorschriften vorzusehen (Daniel Jositsch, Grundriss des schweizerischen Strafprozessrechts Zürich/St. Gallen, 2009, N 21).

162 Amendment IV: *«The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.»*

163 Lothar Determann, Datenschutzrecht in den USA (§ 33), in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Zürich 2015, 1157 ff., Rn. 33.9.

164 Wex, Legal Information Institute (LII), Fourth Amendment, <www.law.cornell.edu/wex/fourth_amendment> (zuletzt besucht am 18. November 2016); Rolf H. Weber/Dominic N. Staiger, in: Jusletter IT 15. Mai 2014, 8.

165 E. 94 des Urteils.

166 E. 88 und 93 des Urteils.

167 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, abrufbar unter <www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf> (zuletzt besucht am 18. November 2016). Der USA Patriot Act besteht aus verschiedenen Änderungen bestehender Gesetzgebungen; Weber/Staiger (FN 164), 9.

168 50 U.S. Code Chapter 36, abrufbar unter <www.law.cornell.edu/uscode/text/50/chapter-36/subchapter-I> (zuletzt besucht am 18. November 2016).

169 Gespeicherte Sprachnachrichten können gestützt auf einen Durchsuchungsbefehl herausverlangt werden. Die Voraussetzungen zum Erhalt eines Durchsuchungsbefehls (search warrant) sind deutlich tiefer als die Voraussetzungen für die Erteilung einer Überwachungsermächtigung (surveillance warrant), Wex, Legal Information Institute (LII), Electronic Surveillance, <www.law.cornell.edu/wex/electronic_surveillance> (zuletzt besucht am 18. November 2016).

mieren.[170] Der Patriot Act sieht ferner keine im Einzelfall vorzunehmende Verhältnismässigkeitsprüfung vor (anders als das neue NDG in der Schweiz, siehe oben).

Neben den auf Section 215 des USA Patriot Act beruhenden Verfügungen haben US-Unternehmen die Möglichkeit, freiwillig und ohne Haftungsrisiko in den USA den Behörden eine direkte Verbindung zu den Daten ihrer Kunden zu gestatten. Die Modalitäten der Datenherausgabe werden in solchen Fällen direkt mit den Behörden verhandelt. Aufgrund des Reputationsschadens, welcher den beteiligten Unternehmen durch eine Bekanntgabe an diesem Programm zweifelsohne erwachsen würde, wurde die entsprechende Liste als top-secret eingestuft. Aufgedeckt wurde diese freiwillige Zugangsgewährung zu Kundendaten von Edward Snowden. Weil das Vorgehen auf freiwilliger Basis geschieht, erfolgt sie ohne Ausübung einer richterlichen Kontrolle und ohne Verfügung. Die betroffenen Kunden eines Unternehmens werden zu keinem Zeitpunkt informiert. Gemäss einer Statistik vom Dezember 2009 erfolgten rund 20 % der amerikanischen Überwachungsmassnahmen gestützt auf dieses «freiwillige» System. Weitere 23 % beruhten auf gerichtlichen Verfügungen auf Grundlage des FISA.[171]

Schliesslich nutzen amerikanische Ermittlungsbehörden (insbesondere das Federal Bureau of Investigation) für die Anordnung von Überwachungsmassnahmen sogenannte National Security Letters (NSL). Diese werden direkt von der Ermittlungsbehörde ausgestellt und unterliegen nicht der Genehmigung eines Gerichts, was aus rechtsstaatlicher Sicht sicherlich problematisch ist. Mit National Security Letters können etwa Internet-Provider verpflichtet werden, Randdaten[172] ihrer Kunden zur Verfügung zu stellen, ohne dass diese Kunden darüber informiert werden müssen. National Security Letters sind in der Praxis verbreiteter als durch ein Gericht genehmigte Überwachungen. Gemäss einer Statistik des Electronic Privacy Information Center (EPIC) wurden im Jahre 2010 circa 1'600 Gerichtsbeschlüsse nach dem Foreign Intelligence Surveillance Act (FISA) erlassen, die Zahl der National Security Letters soll dagegen bei rund 24'000 liegen.[173]

Die Beauftragung eines Board Portal Provider, der über in den USA stationierte Server verfügt oder für die Disaster Recovery (Katastrophenwiederherstellung) auf Servern in den USA Backup-Kopien der Inhalte von Board Portalen erstellt, ist demnach mit einer erhöhten Gefahr von Zugriffen durch amerikanische Nachrichtendienste oder Ermittlungsbehörden verbunden.

2.3 Überwachung

Die Fernmeldeüberwachung ist eine Bundeskompetenz und im US Code, Title 18, Part I – Crimes (Chapter 1–123) geregelt (nachfolgend zitiert nach Sections als §§ 1–2725 **«US-StGB»).** Gemäss § 2516 US-StGB sind die folgenden drei Strafverfolgungsbehörden zur Fernmeldeüberwachung ermächtigt: Das Federal Bureau of Investigation oder eine Federal Agency, die investigative or law enforcement officers der Teilstaaten und die für «Federal felonies» zuständigen investigative or law enforcement officers. Für jede dieser drei Arten von Strafverfolgungsbehörden definiert das Gesetz die richterliche Genehmigungsbehörde und den Überwachungen rechtfertigenden Straftatenkatalog anders.[174] Abweichend zur derzeitigen Rechtslage[175] in der Schweiz sind Host-Providers, wie etwa die Board Portal Providers, gestützt auf § 2516 US-StGB bereits jetzt zur Duldung von Überwachungsmassnahmen verpflichtet.[176]

Für das Federal Bureau of Investigation und die Federal Agencies gilt eine umfassende und detaillierte Auflistung von Straftatbeständen mit unterschiedlichen Höchststrafen.[177] Der für die Behörden der Teilstaaten massgebliche Katalog ist dagegen sehr offen formuliert und erfasst u.a. Bestechung, Erpressung, Betäubungsmittelhandel und jede andere für Leib, Leben und Vermögen gefährliche Straftat, auf die eine Freiheitsstrafe von über einem Jahr steht.[178] Schliesslich ist die Überwachung zur Verfolgung jeder «Federal felony» vorgesehen.[179] Als «felony» gilt jede Straftat mit einer angedrohten Höchstsanktion von mehr als einem Jahr Freiheitsstrafe.[180] Der Katalog gemäss Subsection (1) von § 2516 US-StGB, der neben «felonies» auch weniger schwere Straftaten enthält, dient somit – abweichend zur Rechtslage in der Schweiz – weniger der Eingrenzung der strafprozessualen Fernmeldeüberwachung, sondern hat seine Ursache primär in einer Kompetenzabgrenzung.[181]

Vergleichbar mit der Rechtslage in der Schweiz verlangt die Überwachung gemäss US-StGB – neben einem dringenden Tatverdacht[182] in Bezug auf eine der in § 2516 US-StGB spezifizierten Straftaten – die Subsidiarität

---

170 Weber/Staiger (FN 164), 9 f.

171 Weber/Staiger (FN 164), 12; The New York Times in collaboration with Tagesanzeiger, No Morsel Too Minuscule for All-Consuming N.S.A., 2. November 2013, abrufbar unter <www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html> (zuletzt besucht am 18. November 2016).

172 Der eigentliche Übertragungsinhalt einer Kommunikation, wie beispielsweise die Diskussion im VR anlässlich einer Video-Konferenz, ist jedoch nicht erfasst.

173 Arnd Böken, Patriot Act und Cloud Computing – Zugriff auf Zuruf?, abrufbar unter <www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html> (zuletzt besucht am 18. November 2016).

174 BSK StPO-Jean-Richard-Dit-Bressel, Art. 269 N 54.

175 Mit Inkrafttreten des neuen Büfs wird dies auch in der Schweiz möglich sein (siehe oben 1.3a).

176 § 2518 (4)(e) US-StGB.

177 Subsection (1) von § 2516 US-StGB.

178 Subsection (2) von § 2516 US-StGB.

179 Subsection (3) von § 2516 US-StGB.

180 18 USC § 3559 (a).

181 BSK StPO-Jean-Richard-Dit-Bressel, Art. 269 N 54.

182 18 USC § 2518 (3) (c).

als Anordnungsvoraussetzung, die sehr ähnlich wie in Art. 269 Abs. 2 lit. c StGB definiert ist.[183]

2.4 Datenzugriff aufgrund des Stored Communications Act

Amerikanische Behörden[184] können gestützt auf den Stored Communications Act (SCA)[185] die Offenlegung elektronisch gespeicherter Kundendaten bei elektronischen Kommunikationsdiensten beantragen. Die Offenlegung kann dabei sowohl die Zwischenspeicherung wie auch eine Backup-Speicherung von auf einem Server gespeicherten Kommunikationsinhalten[186] zum Gegenstand haben. Ähnlich wie unter Schweizer Recht ist auch hier zu unterscheiden zwischen dem Zugriff auf den eigentlichen Kommunikationsinhalt oder nur auf Randdaten (wie z.B. Namen und Adressen der Kommunizierenden oder Zeit und Dauer einer Kommunikation).

Es bestehen verschiedene Möglichkeiten für US-Behörden, um auf den Kommunikationsinhalt von Board Portalen[187] zugreifen zu können.[188] Zunächst kann ein «Warrant» erwirkt werden. Warrants werden i.d.R. durch einen Vollstreckungsbeamten vollzogen. Bei Warrants, die zur Offenlegung von bei Host-Providern gespeicherten Inhalten von Dritten verpflichten, werden jedoch ausnahmsweise die entsprechenden Provider direkt zur Offenlegung aufgefordert.[189] Die im vorliegendem Kontext relevanten Voraussetzungen für die Erteilung eines Warrant sind: Einreichung eines Affidavit sowie Nachweis eines Verbrechens.[190] Nicht nötig ist hier, dass der Kunde bzw. der VR vorgängig informiert wird.[191] Eine Befolgung des Verhältnismässigkeitsprinzips im Einzelfall scheint der Stared Communications Act nicht exziplit vorzusehen.

Daneben können die Informationen mittels *Subpoena* oder einem speziellen «Court Order» gemäss § 2703 (d) US-StGB erlangt werden.[192] In beiden Fällen ist der Kunde bzw. der VR jedoch vorgängig zu informieren.[193]

Die Vollstreckung einer *Subpoena* erfolgt grundsätzlich nicht durch einen Vollstreckungsbeamten (und setzt auch nicht dessen Teilnahme voraus). Vielmehr richtet sie sich direkt an die betroffene Person (z.B. einen Board Portal Provider), mit der Aufforderung, Informationen unter Strafandrohung auszuhändigen.

Der Court Order gemäss § 2703 (d) US-StGB ist eine Mischform zwischen Warrant und *Subpoena*. Hierbei muss die Behörde bei einem Gericht «specific and articulable facts» vorbringen, welche hinreichende Gründe für die Annahme liefern, dass die verlangten Daten für den weiteren Verlauf einer Strafuntersuchung wesentlich sind.[194] Wenn das Gericht dies bejaht, unterzeichnet es diesen «Court Order». Der Order wird dann wie eine normale *Subpoena* an den Board Portal Provider zugestellt.[195] Der Board Portal Provider liefert hierauf die Informationen an die Behörde. Die Voraussetzungen der Erteilung einer *Subpoena* gestützt auf § 2703 (b) (B) (i) US-StGB sind tief. Verlangt ist lediglich, dass die anfragende Behörde einen Zusammenhang zwischen einer strafbaren Handlung und dem Inhalt (eines Board Portals) nachweist.[196]

Auf die Randdaten kann mittels Warrant, Court Order gemäss § 2703 (d) US-StGB oder *Subpoena* zugegriffen werden.[197] Hierbei ist es bei keiner dieser Zugriffsmöglichkeiten notwendig, dass der Kunde vorgängig informiert wird.[198] Anders als in der Schweiz besteht keine Beschränkung hinsichtlich des Zugriffs auf Randdaten auf 6 Monate.

2.5 Extraterritoriale Datenbeschaffung durch US-Behörden

In einem erst kürzlich ergangenen Urteil (14. Juli 2016)[199] hat der US Court of Appeals for the Second Circuit entschieden, dass Microsoft Corporation (USA) nicht verpflichtet ist, aufgrund einer strafprozessualen Anordnung der US-Regierung (Warrant) E-Mails von Kunden herauszugeben, die ausschliesslich auf Servern in Irland

---

183 «[…] *normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;* […].»

184 Diese umfassen auf Bundesebene den US Attorney General und das FBI. Daneben können aber auch die FDA, der IRS, die SEC und die FTC Beschlagnahmungen gestützt auf den SCA anordnen.

185 Kodifiziert in Chapter 121, §§ 2701–2712. Der SCA ist ein Abschnitt des Electronic Communications Privacy Act (ECPA).

186 § 2510 (17) (b) US-StGB.

187 Board Portal Provider sind grundsätzlich als remote computing service gemäss § 2711 (2) US-StGB zu qualifizieren. § 2711 (2): *«[…] the term «remote computing service» means the provision to the public of computer storage or processing services by means of an electronic communications system; […].»* Wenn Board Portal Provider auch Kommunikationsdienstleistungen anbieten (wie E-Mail, Chat, oder Internet-Telefon), gelten sie zusätzlich als sog. «electronic communication service» gemäss § 2703 (a) US-StGB, für welche spezielle Eingriffsvoraussetzungen vorgesehen sind; H. Marshall Jarrett/Michael W. Bailie, Office of Legal Education, Executive Office for United States Attorneys, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (manual), 120, abrufbar unter <www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf> (zuletzt besucht am 18. November 2016).

188 § 2703 (b) US-StGB.

189 Marsha/Bailie (FN 187), 134.

190 Marsha/Bailie (FN 187), 134. Es gelten grundsätzlich die Voraussetzungen von Rule 41 (Search und Seizure) der Federal Rules of Criminal Procedure.

191 § 2703 (b) (1) (A) US-StGB.

192 § 2703 (b) (1) (B) US-StGB.

193 § 2703 (b) (1) (B) US-StGB.

194 § 2703 (d).

195 Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review 2005, 1219.

196 Marsha/Bailie (FN 187), 128 f.

197 § 2703 (c) US-StGB.

198 § 2703 (c) (3) US-StGB.

199 *Microsoft Corp. v. USA*, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (2d Cir. July 14, 2016) (Docket No. 14-2985).

gespeichert sind, welche von der irischen Tochtergesellschaft der Microsoft Corporation (USA) betrieben werden. Aufgrund dieser E-Mails erhoffte sich die US-Regierung, an Informationen betreffend einer strafbaren Handlung (Drogenhandel) zu gelangen. Weil auf die E-Mails des Kunden ausschliesslich in Irland zugegriffen werden konnte, hätte die Verpflichtung zur Herausgabe eine extraterritoriale Datenbeschaffung dargestellt. Der Court of Appeals vertrat die Auffassung, dass die Warrant-Bestimmungen des Stored Communications Act eine solche extraterritoriale Anwendung nicht erlauben würden. Der Kongress habe nicht die Absicht gehabt, dass die vom SCA gedeckten Warrants extraterritorial gelten sollen. Um an ausserhalb der USA liegende Daten gelangen zu können, müsse grundsätzlich der Rechtshilfeweg («mutual legal assistance») bestritten werden.[200]

Der Court of Appeals sprach sich im Urteil aber nicht grundsätzlich gegen eine extraterritoriale Datenbeschaffung durch US-Behörden aus. Eine solche sei vielmehr möglich, wenn der Kongress explizit zum Ausdruck bringe, dass einem bestimmten Erlass extraterritoriale Wirkung zukommen soll.[201] Extraterritoriale Wirkung können insbesondere *Subpoenas* haben bzw. Gesetze, die die Möglichkeit der Gewährung von *Subpoenas* einräumen. Hinzuweisen ist in diesem Zusammenhang auf eine im Mai 2016 vorgestellte Gesetzesinitiative (International Communications Privacy Act, ICPA), die den Electronic Communications Privacy Act (ECPA) ergänzen soll. Der derzeit aktuelle Entwurf[202] sieht ausdrücklich vor, dass unter bestimmten Umständen[203] die elektronischen Kommunikationsinhalte sowohl von ausländischen wie auch von US-amerikanischen Kunden, unabhängig davon, wo diese gespeichert sind (d.h. auch ausserhalb der USA), von US-Kommunikationsdiensten (insbes. Internet-Service Provider) an US-Ermittlungsbehörden herausgegeben werden müssen.

Selbst wenn ein US Board Portal Provider die Board Portal-Inhalte ausschliesslich in Rechenzentren ausserhalb der USA speichert, kann somit im Falle des Inkrafttretens des ICPA nicht ausgeschlossen werden, dass US-Ermittlungsbehörden zukünftig über US-Kommunikationsdienste darauf Zugriff erhalten werden.

VI. Wirtschaftlicher Nachrichtendienst (Art. 273 StGB)?

Nach Art. 273 StGB ist u.a. strafbar, wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle zugänglich macht.[204] Die Informationen auf einem Board Portal beinhalten fraglos Geschäftsgeheimnisse des betreffenden Unternehmens und zumindest teilweise auch von Dritten. Man könnte nun argumentieren, dass die Benutzung eines Board Portals mit Servern in einem Land mit unzureichendem Datenschutz bzw. umfassenden Zugriffsmöglichkeiten der Behörden unter diesen Tatbestand fallen würde.[205] Dies mit der Argumentation, dass man damit eventualvorsätzlich in Kauf nimmt, einem fremden Staat die Geheimnisse zugänglich zu machen.[206] Dies ist insbesondere relevant hinsichtlich Geheimnissen, bei denen eine Drittperson und nicht das Unternehmen der Geheimnisherr ist oder bei denen unmittelbar staatliche Interessen betroffen sind.[207]

Diese Auslegung würde wohl unter geltendem Rechtsverständnis zu weit gehen.[208] Die Benutzung eines ausländischen Servers gilt normalerweise trotz der teilweise weitgehenden Zugriffsrechte im Ausland (insbesondere der USA) noch nicht als «zugänglich machen». Ferner werden die Verantwortlichen i.d.R. nicht damit rechnen, dass die Informationen wohl zu ausländischen Behörden gelangen könnten, und dies dann in Kauf nehmen.[209] Es ist aber durchaus denkbar, dass in Zukunft sowohl das Bewusstsein der Gefahr eines Datenzugriffs sowie die Zugriffsmöglichkeiten ausländischer Behörden weiter zunehmen werden. Die Anwendung von Art. 273 StGB wäre wohl ernsthaft zu erwägen, wenn diese Entwicklung so weit gediehen wäre, dass man davon ausgehen muss, dass Entscheidungsträger wissen, dass Daten, die

---

200 Siehe Seiten 25 ff. und 39 ff. des Urteils.

201 Seite 23 des Urteils.

202 Abrufbar unter <www.hatch.senate.gov/public/_cache/files/507a24ea-3442-4ff4-958b-f72dfc779824/ALB16525.pdf> (zuletzt besucht am 18. November 2016).

203 Eine Voraussetzung der extraterritorialen Datenbeschaffung ist dabei insbesondere, dass das Land, in welchem die Kommunikationsinhalte gespeichert sind, kein sog. «Law Enforcement Cooperation Agreement» mit den USA abgeschlossen hat, in welchem die Prinzipien der Convention on Cybercrime vom 23. November 2001 (abgeschlossen in Zypern) umgesetzt sind.

204 Ausführlich hierzu Markus Husmann, Wirtschaftlicher Nachrichtendienst: Schutz kollektiver Rechtsgüter – Bedrohung für den Einzelnen?, in: Ackermann/Hilf (Hrsg.) Top Secret, Zürich 2015, 59 ff.; Andreas Donatsch/Wolfgang Wohlers, Strafrecht IV – Delikte gegen die Allgemeinheit, 4. Aufl., Zürich 2011, 342 ff.

205 Siehe zum räumlichen Anwendungsbereich BSK StGB-Husmann, Art. 273 N 78 ff. m.w.H.

206 «Zugänglich machen» erfordert nicht, dass die ausländische Stelle tatsächlich Kenntnis vom Geheimnis erlangt; Donatsch/Wohlers (FN 189), 347.

207 Wenn das Unternehmen Geheimnisherr ist, kann es einwilligen, womit der Geheimhaltungswille entfällt. Anders liegt der Fall aber dann, wenn die relevanten Informationen unmittelbar staatliche Interessen betreffen, die der Disposition des einwilligenden Unternehmens entzogen sind; Donatsch/Wohlers (FN 204), 349 m.w.H.; Günter Stratenwerth/Felix Bommer, Schweizerisches Strafrecht – Besonderer Teil II, Straftaten gegen Gemeininteressen, 7. Aufl., Bern 2013, 301.

208 Husmann (FN 204), 82.

209 Anders läge wohl der Fall, wenn bewusst ein ausländischer Cloud-Betreiber benutzt würde, damit ausländische Behörden die Wirtschaftsgeheimnisse einsehen kann. Dies wird in der Praxis aber kaum je geschehen.

ins Ausland geliefert werden, auf dem Pult der entsprechenden Behörden landen.[210]

VII. Fazit

Board Portale sind ein wertvolles Instrument, um die Tätigkeit von Verwaltungsräten effizienter zu gestalten. Dies ist gerade hinsichtlich der stetigen Bestrebung, die Corporate Governance zu verbessern, eine nicht zu unterschätzende Hilfe. Wie bei jeder Innovation stellt sich auch hier eine Vielzahl von Rechtsfragen aus einem Potpourri betroffener Rechtsgrundlagen.

Aus gesellschaftsrechtlicher Sicht ist die Willensbildung mittels der Möglichkeiten der Board Portale prinzipiell zulässig. Bei Telefon- und Videokonferenzen besteht hierbei aus unserer Sicht auch kein Vetorecht der einzelnen Mitglieder. Hinsichtlich der Beschlussfassung mittels E-Mail und Chat besteht ein solches Vetorecht. Es ist ferner bezüglich dieser Beschlussformen zu empfehlen, dass Board Portale die Möglichkeit einer elektronischen Unterschrift gewähren. Dies mag allenfalls *de lege ferenda* nicht mehr nötig sein. In jedem Fall ist empfehlenswert, diese Beschlussformen im Organisationsreglement zu verankern. Der Entwurf der Aktienrechtsrevision stellt nun explizit klar, dass die Beschlussfassung mittels elektronischer Mittel zulässig ist. Ein Veto-Recht besteht hierbei, wie unseres Erachtens bereits unter bestehendem Recht, bei E-Mails, aber nicht bei Telefon- und Videokonferenzen. Gemäss dem Entwurf scheint ferner die Durchführung einer virtuellen VR-Sitzung neu nur bei einer Grundlage in den Statuten zulässig zu sein. Dies ist praktisch nicht zweckmässig und aus rechtlicher Sicht ein Systembruch hinsichtlich der Kompetenzaufteilung in der AG. Der Entwurf sollte dementsprechend angepasst werden und auf dieses Erfordernis verzichten (siehe den Vorschlag unter III. 3.).

Von erheblicher Bedeutung sind ferner Fragen des Datenschutzes und der Sicherheit der Daten vor Behördenzugriffen. Bei Board Portalen, deren Server sich ausschliesslich in der Schweiz befinden, lassen sich die datenschutzrechtlichen Herausforderungen einfach bewältigen. Solche Schweizer Board Portale erfahren aufgrund von Art. 10a DSG («Bearbeitungsprivileg») sogar eine gewisse Privilegierung.[211] Zu beachten ist hier, dass dann, wenn VR-Mitglieder von einem Land mit nicht angemessenem Datenschutz auf das Board Portal zugreifen (z.B. von den USA aus), die abgerufenen Informationen nicht auf die mobilen Endgeräte heruntergeladen werden können.

Die Beauftragung eines Board Portals, welches (auch) im Ausland stationierte Server verwendet, ist hingegen aufgrund der damit einhergehenden Übermittlung von Personendaten immer dann mit Risiken behaftet, wenn das Land, in dem der Server steht, über keinen angemessenen Datenschutz verfügt. Letzteres ist gemäss schweizerischer wie auch europäischer Auffassung insbesondere betreffend die USA, einem beliebten Standort für Board Portal Provider, der Fall. Die rechtmässige Übermittlung von Personendaten von der Schweiz/EU in die USA muss deshalb entweder basierend auf der Einwilligung der betroffenen Personen oder Datenübermittlungsverträgen (Musterverträge, EU-Standardvertragsklauseln) erfolgen. Beide Varianten sind mit praktischen Umsetzungsproblemen behaftet (Verweigerung/Widerruf der Einwilligung bzw. Verweigerung des Abschlusses eines Datenübermittlungsvertrags). Erschwerend kommt hinzu, dass derzeit fraglich ist, ob die anerkannten EU-Standardvertragsklauseln und Musterklauseln in Zukunft eine rechtmässige Grundlage für den transatlantischen Datenaustausch bilden.

Weil in den meisten EU-Staaten die Personendaten juristischer Personen nicht geschützt sind, begründet die Beauftragung eines Board Portal Providers mit Servern in der EU eine Datenbekanntgabe ins Ausland mit ungenügendem Datenschutz. Diese Bekanntgabe bedarf grundsätzlich ebenfalls eines besonderen Rechtfertigungsgrundes, wie insbesondere eines Datenübermittlungsvertrags zwischen der Gesellschaft und dem Board Portal Provider.

Board Portale bewirken, dass keine oder zumindest viel weniger Papierausdrucke von VR-Unterlagen erstellt werden, welche dann schwer kontrollierbar zirkulieren. Dies ist hinsichtlich der Datensicherheit zu begrüssen. Andererseits stellt sich das Problem, dass sensitive Daten[212] an einem Ort konzentriert werden, und insbesondere staatliche Behörden mit immer effektiveren technischen Mitteln auf diese Daten zugreifen möchten.

Hinsichtlich des Zugriffs von Schweizer Behörden hat die Analyse ergeben, dass die Risiken überschaubar sind. Im Vergleich zu herkömmlichen VR-Sitzungen bzw. Papierunterlagen besteht neu insbesondere die Möglichkeit der Überwachung durch Strafverfolgungsbehörden und allenfalls gar des Nachrichtendienstes. Diese werden aber in der Praxis kaum relevant werden für VRs. Die

---

210 Zu erwägen wäre auch die Anwendung von Art. 271 StGB. Diesbezüglich ist die Gefahr, dass der Straftatbestand vorliegt jedoch geringer, da hier ein engerer Konnex zur staatlichen Handlung vorliegen muss. Die Übermittlung von Informationen an Private (wie Board Portal Provider) ins Ausland ist nicht schon dann von Art. 271 erfasst, wenn sie in der Folge einer ausländischen Behörde zugänglich werden, sondern nur wenn sie gerade zu diesem Zweck übermittelt wurden; BSK StGB-Husmann, Art. 271 N 64 m.w.H.; vgl. auch BSK StGB-Husmann, Art. 273 N 80 m.w.H.

211 Insbesondere muss die mit der Beauftragung eines Board Portals einhergehende Weitergabe von Personendaten an den Board Portal Provider bei der Beschaffung der Personendaten den betroffenen Personen nicht erkennbar gemacht werden.

212 Personendaten, Fabrikations- und Geschäftsgeheimnisse etc.

Voraussetzungen einer Überwachung sind dergestalt, dass ein VR nur in absoluten Ausnahmefällen in eine Untersuchung involviert sein wird und dann meistens auch nicht als beschuldigte Partei. Das Erfordernis einer gerichtlichen Genehmigung stellt zudem sicher, dass sich die Behörden auch an diese Voraussetzungen halten. Hinsichtlich der Beschlagnahme gelten im Wesentlichen die gleichen Regeln wie bei herkömmlichen VR-Unterlagen in Papierform.

Anders verhält sich die Situation bei Board Portal Providern mit Sitz in den USA. Wählt eine Gesellschaft mit Sitz in der Schweiz bzw. der EU einen solchen Provider, muss sie viel eher damit rechnen, dass amerikanische Behörden, insbesondere die Geheimdienste, auf praktisch alle Daten, die in die USA transferiert werden, zugreifen können. Oftmals geschieht dies auch ohne gerichtliche Genehmigung oder sogar aufgrund einer Kooperation amerikanischer Internet-Provider mit amerikanischen Behörden. Hier scheinen sich die Auffassungen darüber, was verhältnismässige Eingriffe in Grundrechte sind, diesseits und jenseits des Atlantiks relativ stark zu unterscheiden. Hierbei muss fairerweise aber auch gesagt werden, dass sich die Schweiz mit der Annahme des neuen Nachrichtendienstgesetzes (NDG) zumindest ein Stück weit der nachrichtendienstlichen Situation in den USA angenähert hat.

Hinsichtlich Überwachungsmassnahmen und Beschlagnahmungen, die einen konkreten Tatverdacht voraussetzen, scheinen sich die Eingriffsvoraussetzungen in den USA nicht wesentlich von denjenigen in der Schweiz zu unterscheiden. Nennenswert ist jedoch, dass der Deliktskatalog, welcher Überwachungsanordnungen und Beschlagnahmungen rechtfertigt, in den USA um einiges umfangreicher ist, als in der Schweiz. Zudem scheint der für die Offenlegung elektronisch gespeicherter Daten relevante Stored Communications Act keine im Einzelfall vorzunehmende Verhältnismässigkeitsprüfung vorzusehen.

Schliesslich ist auf den geplanten International Communications Privacy Act (ICPA) hinzuweisen, welcher US-Ermittlungsbehörden unter bestimmten Voraussetzungen berechtigt, ausserhalb der USA gespeicherte elektronische Inhalte bei US-Kommunikationsdiensten[213] anfordern können. Die Kommunikationsinhalte können dabei sowohl von US-amerikanischen wie auch ausländischen Kunden stammen.

Die Analyse der verschiedenen Rechtsquellen ergibt somit das relativ überraschende Resultat, dass sich neben dem klassischen Qualitätsstandard «Made in Switzerland» ein neuer rechtlicher Standard herausbildet. «Hosted in Switzerland» kann dem VR aus rechtlicher Sicht das Leben deutlich erleichtern.

---

213 Dazu sind auch Board Portal Provider zu zählen.