

Recht im digitalen Zeitalter

Festgabe Schweizerischer Juristentag 2015 in St. Gallen

Herausgegeben im Auftrag der Rechtswissenschaftlichen Abteilung
der Universität St. Gallen von

Lukas Gschwend
Peter Hettich
Markus Müller-Chen
Benjamin Schindler
Isabelle Wildhaber



Das Kunstwerk auf dem Umschlagbild stammt von Felice Varini «Dix disques évidés plus neuf moitiés et deux quarts», 2014, Acryl und Folien. Es befindet sich im Bibliotheksgebäude der Universität St. Gallen.

Abgedruckt mit freundlicher Genehmigung des Künstlers. Das Copyright liegt bei Felice Varini und der Universität St. Gallen (HSG).

Fotografie: Hannes Thalmann

Bibliografische Information der «Deutschen Bibliothek».

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Alle Rechte, auch des Nachdrucks von Auszügen, vorbehalten. Jede Verwertung ist ohne Zustimmung des Verlages unzulässig. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronische Systeme.

© Dike Verlag AG, Zürich/St. Gallen 2015
ISBN 978-3-03751-708-6

www.dike.ch

Verwaltungsrat im digitalen Zeitalter

ROLAND MÜLLER

Inhaltsübersicht

I.	Problemübersicht	249
1.	Steigende IT-Anforderungen an den Verwaltungsrat	249
2.	Notwendige IT-Entscheidungen auf Stufe Verwaltungsrat	250
II.	Auswirkungen auf die Aufgaben des Verwaltungsrates	251
1.	Auswirkungen auf die Pflicht zur Oberleitung	251
2.	Auswirkungen auf die Pflicht zur Organisation	254
3.	Auswirkungen auf die Pflicht zur Finanzplanung und Finanzkontrolle	255
4.	Auswirkungen auf die Besetzung und Beaufsichtigung der Geschäftsführung	258
5.	Auswirkungen auf die Pflicht zur Durchführung der Generalversammlung	259
6.	Auswirkungen auf die Pflicht zur Richterbenachrichtigung bei Überschuldung	260
III.	Verwaltungsrat und Datenschutz	261
1.	Datenschutzrechtliche Pflichten des Verwaltungsrates	261
2.	Problematische Bereiche	263
a)	Übersicht	263
b)	Biometrie	263
c)	Grenzüberschreitende Datenspeicherung	266
3.	Folgen einer datenschutzrechtlichen Verletzung	268
IV.	Zusammenfassung und Empfehlungen	270

I. Problemübersicht

1. Steigende IT-Anforderungen an den Verwaltungsrat

Seit der grossen Aktienrechtsreform 1992 haben die Anforderungen an Verwaltungsräte in der Schweiz markant zugenommen. Der Katalog an unentziehbaren und undelegierbaren Aufgaben gemäss Art. 716a OR wird von Lehre und Rechtsprechung immer extensiver ausgelegt.¹ Es erstaunt daher nicht, dass auch die jährliche Zahl der Verantwortlichkeitsklagen gegen Verwaltungsräte laufend ansteigt.² Zwei Faktoren beeinflussen dabei die Arbeit der Verwaltungsräte zusätzlich: die Überregulierung und die Digitalisierung. Während der Regulierungsflut bewusst mit immer wirksame-

¹ Vgl. dazu die ausführliche Liste der Aufgaben des Verwaltungsrats bei MÜLLER ROLAND/LIPP LORENZ/PLÜSS ADRIAN, Der Verwaltungsrat, 4. Aufl. Zürich 2014, S. 798 ff.

² Dies zeigt die Studie von KELLER SUSANNE, Verantwortlichkeit des Verwaltungsrates, in: Jusletter vom 24. Oktober 2011.

ren Mittel zur Einhaltung der Compliance begegnet wird,³ fehlt es den Verwaltungsräten vielfach noch am Bewusstsein um die Chancen und Risiken der fast vollständigen Digitalisierung der weltweit gespeicherten Informationsmenge. Die massenhafte Sammlung, Speicherung und Übertragung digitaler Daten ist für die strategische Führungsebene jedes Unternehmens eine extreme Herausforderung in mehrfacher Hinsicht. Die nun vorhandenen Möglichkeiten zur Überwachung von Menschen, Maschinen und Prozessen können positiv zur Fokussierung und zur Beschleunigung der Geschäftstätigkeit genutzt werden. Gleichzeitig steigt aber die Gefahr der Verletzung des Rechts auf Privatsphäre bei allen Mitarbeitern und die Bedrohung durch konkurrierende oder gar schädigende Eingriffe von dritter Seite nimmt exponentiell zu.

Während früher VR-Mitglieder oft darüber klagten, sie hätten zu wenige Informationen von der Geschäftsleitung, ist heute das Gegenteil der Fall. Es gibt zu viele «Tools», welche auf Knopfdruck unzählige Auswertungen von Daten generieren. Das Speichern von Daten ist heute kein Thema mehr, dafür die Auswahl der relevanten Daten und die Vernichtung unnötiger Daten.⁴ In vielen Unternehmen hat der VR-Sekretär die relevanten Dokumente nicht mehr physisch, sondern elektronisch im VR-Intranet bereitzustellen bzw. zu aktualisieren. An den VR-Sitzungen haben die Teilnehmer nur noch wenig Papier vor sich, dafür den Laptop oder das iPad. Der jederzeitige Zugang zu Daten und die Pflicht zur dauernden Erreichbarkeit erhöhen zweifellos den Arbeitsdruck der Verwaltungsräte.

2. Notwendige IT-Entscheidungen auf Stufe Verwaltungsrat

Um mit den Chancen und Risiken der Digitalisierung erfolgreich umzugehen, muss der Verwaltungsrat zwingend Entscheidungen fällen. Dazu gehören vorab IT-Organisations- und Investitionsentscheide zu folgenden Fragen:

- Soll das IT-Wissen im Unternehmen selbst aufgebaut werden oder sollen externe Provider diese Aufgabe übernehmen?
- Welche Hard- und Software soll konkret angeschafft werden?
- Wo sollen die Daten gespeichert und gesichert werden?
- Wie können die vorhandenen IT-Tools im Unternehmen genutzt werden?

³ So liefert beispielsweise die ISO Norm 19600, publiziert 2014, Empfehlungen zum Aufbau, zur Entwicklung, zur Implementierung, zur Evaluation und zur Optimierung eines effektiven Compliance Management Systems.

⁴ Deshalb sollte jeder Verwaltungsrat in einem MIS-Konzept strukturiert festlegen, welche Informationen von wem in welcher Form wann geliefert werden müssen; vgl. dazu das Muster bei MÜLLER/LIPP/PLÜSS (Fn. 1), S. 939 f.

- Wer soll letztlich in welcher Form zu welchen Daten Zugang haben?
- Wie kann die Datensicherung und die Datensicherheit gewährleistet werden?
- Welche Wege gibt es, um aus der Datenarchivierung den grössten Nutzen zu ziehen?

Meist fehlt auf Stufe Verwaltungsrat das technische Wissen und Verständnis zur Behandlung von diesen IT-Problemen. Es ist deshalb unerlässlich, dass der Verwaltungsrat erfahrene und seriöse IT-Berater bezieht, um die anstehenden Entscheide nach sorgfältiger Abwägung aller Varianten fällen zu können. Bei allen IT-Entscheiden sollte konsequent eine einheitliche Strategie verfolgt werden. Konkret können folgende strategischen IT-Ziele anvisiert werden:⁵

- Unterstützung der Business-Prozesse
- Förderung der Wirtschaftlichkeit bzw. Reduktion der Kosten
- Standardisierung und dadurch Effizienzsteigerung
- Verbesserung der IT Service Delivery

II. Auswirkungen auf die Aufgaben des Verwaltungsrates

1. Auswirkungen auf die Pflicht zur Oberleitung

Gemäss Art. 716a Abs. 1 Ziff. 1 OR hat der Verwaltungsrat die Pflicht zur Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen. Diese strategische Hauptaufgabe kann im Hinblick auf die IT-Problematik in folgende Detailaufgaben unterteilt werden:⁶

- Festlegung der IT-Strategie mit konkreten IT-Zielen
- Analyse von Stärken und Schwächen, Gefahren und Chancen der IT
- Wahl der Mittel und Ressourcen, um die IT-Strategie umzusetzen
- Erteilung von Weisungen an die Geschäftsleitung zur Umsetzung der IT-Strategie
- Sicherstellung, dass bei jeglicher IT-Nutzung stets alle gesetzlichen, statutarischen und reglementarischen Vorschriften befolgt werden (IT-Compliance)
- Festlegung der IT-Personalpolitik
- Erlass einer Risk Management Policy unter Berücksichtigung von IT-Risiken
- Sicherstellung der notwendigen Lizenzen zur IT-Nutzung

⁵ WYSER JÜRIG/WÖLL PETER, IT-Kosten und IT-Performance, Betriebswirtschaftliche Studie der Schweizer Informatikabteilungen, Ernst & Young (Hrsg.), Zürich 2002, S. 5.

⁶ In Anlehnung an die Liste der VR-Aufgaben bei MÜLLER/LIPP/PLÜSS (Fn. 1), S. 798 ff.

- Vorgabe von Grundsätzen des IT-Vertragsmanagements
- Entscheid über den Abschluss wichtiger IT-Verträge (z.B. Outsourcing)
- Abhaltung von VR-Sitzungen mit den erforderlichen IT-Traktanden
- Mindestens einmal jährlich kritische Diskussion der aktualisierten Master Risk List unter Berücksichtigung der IT-Risiken
- Mindestens einmal jährlich Überprüfung der Versicherungssituation auf Grund einer aktualisierten Versicherungsübersicht inkl. Versicherung der IT-Infrastruktur

Der Verwaltungsrat kann zur Erledigung dieser Aufgaben nicht nur auf die Mithilfe der Geschäftsleitung zurückgreifen, sondern auch gezielt VR-Ausschüsse einsetzen.⁷ Nur sehr selten ist in der Praxis ein eigentlicher IT-Ausschuss anzutreffen. Sehr häufig werden dagegen die IT-Aufgaben dem Audit-Committee zugewiesen. Dabei ist zu beachten, dass sich der Verwaltungsrat seiner IT-Verantwortung durch eine solche Delegation nicht entziehen kann. Er bleibt für die sorgfältige Erledigung der undelegierbaren Aufgaben nach Art. 716a i.V.m. 717 OR verantwortlich und kann auch schon bei einer leichten Verletzung seiner entsprechenden Pflichten gestützt auf Art. 754 OR eingeklagt werden.⁸

Im Zusammenhang mit der Pflicht zur Oberleitung des Unternehmens ist das Risk Management für den Verwaltungsrat von besonderer Bedeutung. Unabhängig von Grösse und Branche sind heute alle Unternehmen mit IT-Risiken konfrontiert. Der Verwaltungsrat muss deshalb sicherstellen, dass diese Risiken erfasst, analysiert und entsprechend den Prioritäten mitigiert werden. Dazu kann er dem IT-Verantwortlichen im Unternehmen folgenden Fragenkatalog unterbreiten:

Erneuerungsbedarf

- Wie lange wird die bestehende Hard- und Software den Anforderungen des Betriebes einerseits und der Kunden andererseits noch genügen?
- Welche finanziellen Konsequenzen entstehen bei Ersatzanschaffungen?

Lizenzkontrolle

- Wird nur rechtlich zulässige Originalsoftware eingesetzt?
- Sind genügend Lizenzen für alle Anwender vorhanden?

⁷ Zur Bedeutung und Zusammensetzung von VR-Ausschüssen vgl. MÜLLER ROLAND, HR-Committees – Bedeutung von Nominierungs- und Entschädigungsausschüssen auf Stufe Verwaltungsrat, in: AJP 3/2013, S. 315 ff.

⁸ Dazu ausführlich MÜLLER ROLAND, Unsorgfältige Führung eines Verwaltungsratsmandates, in: Handbücher für die Anwaltspraxis, Bd. V, Peter Münch/Stefan Weber (Hrsg.), 2. Aufl. Basel 2015, S. 975 ff.

Supportkontrolle

- Ist der zukünftige Support gewährleistet?
- Kann bei einem Ausfall der Entwicklungs- oder Supportunternehmen genügend rasch Ersatz beschafft werden?

Datenerfassung

- Welche Risiken resultieren aus fehlerhaften Dateneingaben?
- Sind alle Massnahmen getroffen, um fehlerhafte Dateneingaben zu vermeiden?

Datenarchivierung

- Werden die archivierten Daten genügend lange aufbewahrt?
- Können die archivierten Daten zukünftig noch verwertet werden?

Datensicherung

- Werden sämtliche relevanten Daten gesichert?
- Erfolgt die Sicherung zeitlich genügend häufig?
- Werden die gesicherten Daten genügend geschützt aufbewahrt?
- Werden periodische Kontrollen der gesicherten Daten durchgeführt?

Datensicherheit

- Ist ein ausreichender Schutz gegen Datenzugriff von aussen gewährleistet?
- Besteht eine zuverlässige Kontrolle der Passwörter?
- Werden die Passwörter periodisch ausgewechselt?
- Erfolgt die Weitergabe von Daten an Dritte auf eine ausreichend geschützte Weise?

Geräteausfall

- Besteht eine Alternative bei Stromausfall?
- Wird der Ausfall von einzelnen Hardwarekomponenten automatisch durch andere Geräte kompensiert?
- Wird ein Ausfall der Klimaanlage genügend rasch entdeckt und mittels Ersatzmassnahmen behoben?

IT-Knowhow

- Sind sämtliche relevanten Angaben im Zusammenhang mit der Informatik, insbesondere Hard- und Softwarekomponenten, Datensicherung und Datensicherheit, vollständig schriftlich festgehalten?
- Welcher Knowhow-Verlust resultiert beim Ausfall von Mitarbeitern im IT-Bereich?

IT-Mitarbeiter

- Welchen Schaden können Mitarbeiter aus dem IT-Bereich anrichten, wenn sie Knowhow aus dem IT-Bereich an Dritte weitergeben?
- Ist sichergestellt, dass ein Mitarbeiter aus dem IT-Bereich im Falle seiner Kündigung nicht mehr an den Arbeitsplatz zurück darf?

IT-Vertragsmanagement

- Ist ein Verantwortlicher für die IT-Verträge bestimmt?
- Werden Verträge nur mit klarem Kostendach abgeschlossen?
- Besteht eine angemessene Frist- und Budgetkontrolle?

IT-Projektmanagement

- Besteht eine Übersicht mit Priorisierung der IT-Projekte?
- Ist für jedes Projekt ein Verantwortlicher bestimmt?
- Wurden bei jedem Projekt die notwendigen finanziellen und personellen Ressourcen ermittelt und sind diese gesichert?
- Besteht ein angemessenes Projektreporting?
- Ist sichergestellt, dass neue Projekte nur mit Zustimmung des obersten IT-Verantwortlichen gestartet werden?

IT-Struktur

- Ist die IT-Architektur für die Zukunft ausreichend und bietet sie genügend Entwicklungspotential?
- Sind die verwendeten Datenbanken bezüglich Struktur ausbaufähig und lassen sie sich migrieren?
- Welche Einschränkungen bezüglich Datenmengen und Datenverarbeitung ergeben sich durch die IT-Struktur?
- Werden Standardprogramme verwendet oder gibt es individuelle Anpassungen, welche zukünftige Updates erschweren oder verunmöglichen?

Gestützt auf die konkrete Beantwortung dieser Fragen kann der Verwaltungsrat Entscheidungen im IT-Bereich treffen und sicher sein, dass er dabei die Anforderungen der vom Bundesgericht zu Grunde gelegten Business Judgment Rule berücksichtigt hat.⁹

2. Auswirkungen auf die Pflicht zur Organisation

Um die Oberleitung der Gesellschaft zu verwirklichen, muss das Unternehmen hinreichend organisiert sein.¹⁰ Dazu muss eine Zuteilung von Aufgaben, Kompetenzen und Verantwortung erfolgen. Dies gilt auch für den IT-Bereich. Zur Vermeidung von Doppelspurigkeiten und Unklarheiten hinsichtlich der persönlichen Aufgabenbereiche, ist es erforderlich, stellenbezogene Pflichtenhefte der involvierten Mitarbeiter zu erarbeiten und Über- bzw. Unterordnungen festzulegen. In grösseren Betrieben wird dazu sogar ein eigener Chief Information Officer (CIO) ernannt. Während die Bedeutung des IT-Bereiches ständig weiter zunimmt, sinkt diejenige der CIOs.¹¹ Heute geht es in erster Linie darum, die Effizienz der IT zu steigern.

⁹ Vgl. VOGT HANS-UELI/BÄNZIGER MICHAEL, Das Bundesgericht anerkennt die Business Judgment Rule als Grundsatz des Schweizerischen Aktienrechts, in: GesKR 2012, S. 607 ff.

¹⁰ MÜLLER/LIPP/PLÜSS (Fn. 1), S. 166; FORSTMOSER/MEIER-HAYOZ/NOBEL, Schweizerisches Aktienrecht, Bern 1996, § 30 Rz. 34.

¹¹ DURNSLAFF UWE/LEMP PETER/HEIMANN THOMAS, Studie IT-Trends 2014, Capgemini (Hrsg.), Berlin 2014, S. 5.

Für den Verwaltungsrat ist es im Zusammenhang mit der Organisation sehr wichtig, die Zugriffsberechtigungen festzulegen. Um den immer häufiger werdenden Datendiebstählen vorzubeugen, sollten Mitarbeiter nur soweit Zugriff auf Daten haben, als sie diese zur Ausübung ihrer Funktion benötigen. Gleichzeitig muss auch die Berechtigung der Mitarbeiter zur selbständigen Installation von Software eingeschränkt werden. Nur so kann die Einschleppung von Malware schon von Anfang an verhindert werden. Die Pflicht des Verwaltungsrats zur Festlegung der Organisation kann im IT-Bereich dementsprechend in folgende Detailaufgaben unterteilt werden:¹²

- Bestimmung der Organisationsstruktur des Unternehmens und basierend darauf Festlegung des Organigramms inkl. IT-Abteilung
- Bestimmung des für die Sicherheit im Unternehmen Verantwortlichen (Sicherheitsbeauftragter) und Klarstellung seiner Aufgaben in einem Stellenbeschrieb inkl. IT-Sicherheit
- Erlass eines Organisationsreglements zur Klarstellung von Aufgaben, Kompetenzen und Verantwortlichkeiten innerhalb des Unternehmens inkl. Verantwortlichkeit im IT-Bereich
- Festlegung eines Funktionendiagramms zur Abgrenzung der Kompetenzen von strategischer und operativer Führungsebene inkl. IT-Kompetenzen
- Vorgabe der Führungsinstrumente (MIS-Konzept), um eine ausreichende und rechtzeitige Information des VR sicherzustellen basierend auf der vorhandenen IT-Infrastruktur
- Festlegung der Zeichnungsberechtigungen und falls notwendig, zusätzlich Erlass einer internen Richtlinie zur Unterschriftenregelung insbesondere auch im IT-Bereich
- Im Falle von Namenaktien Aktualisierung und Kontrolle des Aktienbuches unter Verwendung entsprechender IT-Tools
- Vollständige und wahrheitsgemässe Erstellung von Protokollen aller VR-Sitzungen, allenfalls unter Einsatz von entsprechenden Aufzeichnungshilfen und IT-Tools

3. Auswirkungen auf die Pflicht zur Finanzplanung und Finanzkontrolle

Je nach Unternehmensgrösse und Branche ist der IT-Aufwand in einem Unternehmen zur Erreichung der gesetzten strategischen IT-Ziele unterschiedlich hoch; es wird von

¹² In Anlehnung an die Liste der VR-Aufgaben bei MÜLLER/LIPP/PLÜSS (Fn. 1), S. 798 ff.

1–10 % des Umsatzes ausgegangen.¹³ In Unternehmen mit unter 200 Vollzeitangestellten sind 3,5 % davon IT-Mitarbeiter; bei 200 bis 1'000 Vollzeitangestellten sind es bereits 6,9 % und bei über 1'000 Vollzeitangestellten immer noch 6 %.¹⁴ In Banken und Energie-Unternehmen fallen jährlich rund CHF 25'000 bis 30'000 pro Mitarbeiter an IT-Kosten an, bei Unternehmen der Automotive- oder Healthcare-Branche sind es rund CHF 12'000.¹⁵ Die IT-Kosten sind deshalb bei der Budgetierung ein wesentlicher Faktor, welcher vom Verwaltungsrat kritisch zu hinterfragen ist.

Die Pflicht des Verwaltungsrats zur Finanzplanung und Finanzkontrolle kann im IT-Bereich in folgende Detailaufgaben unterteilt werden:¹⁶

- Erlass von Weisungen zur Ausgestaltung des Rechnungswesens inkl. Vorgaben zur Aktivierung und Abschreibung von IT-Hardware und Software
- Sicherstellung einer der Art und dem Umfang der Gesellschaft angemessenen Buchführung, inkl. Vorgabe der zu verwendenden Software
- Sicherstellung der Einhaltung der gesetzlichen Dokumentations- und Aufbewahrungsvorschriften, allenfalls basierend auf elektronischen Archivierungssystemen
- Periodische Genehmigung eines langfristigen Finanzplans inkl. IT-Investitionen, der die Umsetzung des Businessplans sicherstellen soll
- Jährliche Festlegung des Budgets inkl. IT-Investitionsbudget als Grundlage zur Planung und zur Erkennung von Zielabweichungen
- Bestimmung der IT-Provider und Cloud-Anbieter, mit denen das Unternehmen zusammenarbeitet
- Monatliche Überprüfung der vorhandenen und zukünftig benötigten Liquidität (12 Monate rollierender Liquiditätsplan) insbesondere auch im Hinblick auf IT-Investitionen
- Festlegung der notwendigen Rückstellungen beim Jahresabschluss insbesondere für laufende IT-Projekte
- Beurteilung der angemessenen Abschreibungen und Wertberichtigungen im IT-Bereich
- Festlegung von Prüfungsschwergebieten und von der Revisionsstelle speziell zu prüfenden Punkten (ausserhalb der ordentlichen Prüfung der Jahresrechnung) auch im IT-Bereich

¹³ SCHÜLEIN PETER/MURNLEITNER MARTIN, IT-Kosten und Wertmanagement, PricewaterhouseCoopers (Hrsg.), Stuttgart/München 2009, S. 6.

¹⁴ WYSER JÜRG/WÖLL PETER (Fn. 5), S. 9.

¹⁵ In Anlehnung an die Studie von SCHÜLEIN/MURNLEITER (Fn. 7) S. 6.

¹⁶ In Anlehnung an die Liste der VR-Aufgaben bei MÜLLER/LIPP/PLÜSS (Fn. 1), S. 798 ff.

Wie kritisch IT-Investitionen im Hinblick auf die Verantwortlichkeit des Verwaltungsrats sein können, zeigt der Bundesgerichtsentscheid 128 III 92 vom 29. Oktober 2001. In diesem Fall wurde der Verwaltungsrat einer Holdinggesellschaft als faktisches Organ wegen dem Kauf einer teuren Software durch eine Tochtergesellschaft zur Verantwortung gezogen. Konkret war D. seit dem 25. September 1984 einziger Verwaltungsrat der F. AG. Diese erwarb am 24. November 1988 sämtliche Aktien der E. Holding AG, welche ihrerseits alle Aktien der E. AG hielt. Am 24. Februar 1989 wurde D. auch in den Verwaltungsrat der E. AG gewählt. Am 12. Dezember 1988 schlossen die F. AG, die E. AG und die Bank C. eine Vereinbarung zur Sanierung der E. AG. Darin verpflichtete sich die F. AG unter anderem, die Software der E. AG zum Preis von CHF 3'000'000.– zu kaufen. Der Kaufpreis war zur Hälfte bis Ende 1988 zu bezahlen, für die übrigen CHF 1'500'000.– sollte die E. AG der F. AG ein langfristiges Darlehen gewähren. Das Darlehen sollte in jährlichen Raten von CHF 300'000.– amortisiert werden, erstmals per 30. November 1989. Am 5. Juli 1990 wurde aber über die E. AG und die E. Holding AG der Konkurs eröffnet. Die Banken liessen sich von der Konkursmasse die Verantwortlichkeitsansprüche gegen die Organe der konkursiten E. AG abtreten und klagten unter anderen gegen D. auf Bezahlung von CHF 3'000'000.– nebst Zins. Das Bundesgericht kam zum Schluss, D. habe faktisch die E. AG seit deren Übernahme durch die F. AG geleitet bzw. deren Geschäfte geführt. In dieser Eigenschaft habe er pflichtwidrig die Bezahlung des Software-Kaufpreises von CHF 3'000'000.– nicht überwacht bzw. für die kreditierte Kaufpreishälfte keine hinreichenden Sicherheiten vereinbart. Dadurch sei der E. AG ein Schaden in dieser Höhe entstanden, welchen der Beklagte in adäquat kausaler Weise durch die Pflichtverletzung verursacht habe, wofür ihn ein nicht leichtes Verschulden treffe.

Dieser Fall zeigt exemplarisch, dass ein Verwaltungsrat Investitionen im IT-Bereich sorgfältig prüfen und überwachen muss. Wird eine Software in Auftrag gegeben, welche zuerst nach den Bedürfnissen des kaufenden Unternehmens erstellt bzw. adaptiert werden muss, so darf der Kaufpreis nicht sofort ohne Sicherheiten vollständig bezahlt werden. Ansonsten würde von den Gerichten eine Darlehensgewährung zu unüblichen Konditionen angenommen. Zulässig sind in der Praxis Anzahlung von einem Drittel des ganzen Investitionsvolumens. Ein zweiter Drittel kann bei Ablieferung und der letzte Drittel bei Abnahme bezahlt werden. Wenn jedoch der ganze Kaufpreis einer Software sofort bezahlt werden soll, dann muss der Verwaltungsrat auf einer angemessenen Sicherheit (z.B. Bankgarantie) bestehen.

4. Auswirkungen auf die Besetzung und Beaufsichtigung der Geschäftsführung

Auch die Besetzung und Beaufsichtigung der Geschäftsführung hat durch die Digitalisierung grosse Veränderungen erfahren. Dies beginnt bereits bei der Ausschreibung einer vakanten Stelle. Heute werden GL-Mitglieder sinnvollerweise nicht mehr nur über Anzeigen in Printmedien, sondern insbesondere auch auf den einschlägigen Plattformen der Social Media gesucht. Dadurch werden viel mehr potentielle Kandidaten angesprochen als mit dem beschränkten Verbreitungskreis einer Zeitung.

Sind die Bewerbungen physisch oder elektronisch eingegangen, werden die aussichtsreichsten Kandidaten oft mit einer Internetrecherche überprüft. Für die Reputation eines Unternehmens könnten z.B. rassistische Äusserungen oder sexuell anstössige Bilder eines GL-Mitgliedes extrem negative Konsequenzen haben. Ein Verwaltungsrat sollte deshalb sicherstellen, dass die Internetauftritte der aktuellen oder zukünftigen GL-Mitglieder einer kritischen Überprüfung standhalten.

Der Verwaltungsrat kommt seiner entsprechenden Verantwortung im Zusammenhang mit der Bestellung der Geschäftsleitung pflichtgemäss nach, wenn er diesbezüglich das Folgende vorkehrt:¹⁷

- Sorgfältige Auswahl der Geschäftsleitungsmitglieder (*cura in eligendo*)
- Sorgfältige Instruktion der Geschäftsleitungsmitglieder (*cura in instruendo*)
- Sorgfältige Überwachung der Geschäftsleitungsmitglieder (*cura in custodiendo*)

Bei diesen drei Detailaufgaben handelt es sich um einen dauernden Prozess. Der Verwaltungsrat sollte sich also nicht mit der Beurteilung im Zeitpunkt der Anstellung zufrieden geben. Vielmehr muss er periodisch überprüfen, ob die Mitglieder der Geschäftsleitung den aktuellen Aufgaben noch genügen. Dazu sind jährlich konkrete Ziele vorzugeben und entsprechende Evaluationen durchzuführen. Auch dafür gibt es heute entsprechende Software.

Ein wichtiges Hilfsmittel zur Überwachung der Geschäftsführung ist die Einrichtung eines Management Information System (MIS). Dabei handelt es sich um ein technisches Informationssystem basierend auf Datenauswertung. Es stellt dem Verwaltungsrat Informationen zur Verfügung, mit deren Hilfe das Unternehmen gelenkt, bzw. das Controlling betrieben werden kann. Das Management Information System ist der Oberbegriff für höher verdichtete Analysen und Vergleiche. Zielsetzung ist, aus den Datenmengen der operativen Systeme die wesentlichen Führungszahlen auf

¹⁷ MÜLLER/LIPP/PLÜSS (Fn. 1), S. 171; BÖCKLI PETER, Schweizer Aktienrecht, 4. Aufl. Zürich 2009, § 13 Rz. 313.

«Knopfdruck» zu erhalten und damit ein ständig verfügbares Steuerungsinstrument zu schaffen, das dem Management ein frühzeitiges Gegensteuern ermöglicht.¹⁸

5. Auswirkungen auf die Pflicht zur Durchführung der Generalversammlung

Gemäss Art. 716a Abs. 1 Ziff. 6 OR ist der Verwaltungsrat zur Erstellung des Geschäftsberichtes und zur Vorbereitung der Generalversammlung sowie zur Ausführung ihrer Beschlüsse verpflichtet. Bei börsenkotierten Gesellschaften sind durch die Verordnung gegen übermässige Vergütungen (VegüV) vom 20. Januar 2013 zusätzliche Pflichten im Zusammenhang mit der Generalversammlung dazugekommen. Diese neuen Aufgaben wären ohne digitale Unterstützung gar nicht zu bewältigen. So muss der Verwaltungsrat u.a. gemäss Art. 9 VegüV sicherstellen, dass die Aktionäre die Möglichkeit haben, dem unabhängigen Stimmrechtsvertreter zu jedem in der Einberufung gestellten Antrag zu Verhandlungsgegenständen Weisungen zu erteilen, zu nicht angekündigten Anträgen zu Verhandlungsgegenständen sowie zu neuen Verhandlungsgegenständen gemäss Art. 700 Abs. 3 OR allgemeine Weisungen zu erteilen und auch elektronisch Vollmachten und Weisungen zu erteilen.

Der Verwaltungsrat trägt die Verantwortung für die Formulierung des Geschäftsberichtes, bestehend aus Jahresrechnung, Lagebericht und allenfalls Konzernrechnung. Je nach Bedeutung für das Unternehmen sind im Lagebericht auch Angaben zur IT-Infrastruktur zu machen. Bei der Jahresrechnung hat der Verwaltungsrat darauf zu achten, dass insbesondere im IT-Bereich keine übermässige Aktivierung von Eigenleistungen (z.B. Softwareerstellung) stattfindet und dass die betriebswirtschaftlich notwendigen Abschreibungen auf Hard- und Software auch wirklich vorgenommen werden.

Die gesetzliche Frist zur Einladung der Aktionäre zur GV beträgt gemäss Art. 700 Abs. 1 OR mindestens 20 Tage. Dabei stellt sich die Frage, ob die Aktionäre auch elektronisch eingeladen werden dürfen. Da der Gesetzgeber die Form der Einberufung ausdrücklich der statutarischen Regelung vorbehalten hat, ist grundsätzlich auch eine Einberufung per E-Mail möglich.¹⁹

Der Verwaltungsrat hat die Sicherstellung der Zutrittsberechtigung und den Ausschluss von nicht zutrittsberechtigten Personen im Falle eines Widerspruches von Aktionären sicherzustellen. Bei grösseren Aktiengesellschaften mit vielen Aktionären

¹⁸ MÜLLER/LIPP/PLÜSS (Fn. 1), S. 172.

¹⁹ TANNER BRIGITTE, in: Vito Roberto/Hans Rudolf Trüeb (Hrsg.), Handkommentar zum Schweizer Privatrecht – Personengesellschaften und Aktiengesellschaft, 2. Aufl. Zürich 2012, Art. 700 OR Rz. 5.

ist eine solche Kontrolle nur noch unter Einsatz von elektronischen Hilfsmitteln basierend auf einem elektronisch geführten Aktienbuch möglich.

Schliesslich trägt der Verwaltungsrat auch noch die Verantwortung zur korrekten Stimmmittlung inkl. Feststellung der Stimmberechtigung und Bereitstellung von Unterlagen für eine ev. geheime Abstimmung. Auch hier kann eine entsprechende Software bei einer Grossgesellschaft sehr hilfreich sein.

6. Auswirkungen auf die Pflicht zur Richterbenachrichtigung bei Überschuldung

Die letzte unübertragbare und unentziehbare Aufgabe des Verwaltungsrates gemäss Art. 716a Abs. 1 Ziff. 7 OR ist die Pflicht, im Falle der Überschuldung den Richter zu benachrichtigen. Sehr viele Verantwortlichkeitsklagen werden mit einer Verletzung dieser Pflicht begründet.²⁰ Wann ein Kapitalverlust und wann eine Überschuldung im Sinne des Gesetzes vorliegt, definiert Art. 725 OR.

Ein Kapitalverlust im Sinne des Aktienrechts ist dann gegeben, wenn mit dem kumulierten Verlust die Summe von nominellem Aktienkapital und gesetzlichen Reserven mindestens zur Hälfte, aber doch noch nicht vollständig aufgezehrt ist.²¹ Der hälftige Kapitalverlust ist gemäss Gesetz eine kritische Schwelle, bei deren Überschreiten die Aktionäre von der angespannten finanziellen Situation einer Gesellschaft unverzüglich Kenntnis erhalten und über Sanierungsmassnahmen befinden sollen.

Bei einer Überschuldung im Sinne von Art. 725 Abs. 2 OR hat der Bilanzverlust das gesamte Eigenkapital vollständig aufgezehrt. Die vorhandenen, ordnungsgemäss bewerteten Vermögenswerte decken das Fremdkapital (Verbindlichkeiten und Rückstellungen) nur noch teilweise. Man unterscheidet zwischen echter und unechter Überschuldung. Bei der echten Überschuldung ist das Fremdkapital nach Auflösung sämtlicher stillen Reserven nicht mehr durch die Aktiven gedeckt und somit das Eigenkapital effektiv verloren. Im Falle der unechten Überschuldung führt eine Auflösung sämtlicher stillen Reserven dazu, dass die Forderungen Dritter durch das Umlauf- und das Anlagevermögen noch gedeckt sind; das Eigenkapital ist in diesem Sinne nur buchmässig verloren.²²

Die Bewertung der IT-Infrastruktur und insbesondere die Aktivierung von Eigenleistungen im Zusammenhang mit der Erstellung oder Implementierung einer Software

²⁰ Vor Bundesgericht sind es letztlich 47 %; vgl. KELLER (Fn. 2), S. 4.

²¹ Dazu eingehend KÜNG MANFRED/SCHOCH NIKLAUS, in: Heinrich Honsell/Nedim Peter Vogt/Rolf Watter (Hrsg.), Basler Kommentar, Obligationenrecht II, 4. Aufl. Basel 2012, Art. 732a OR Rz. 5.

²² MÜLLER/LIPP/PLÜSS (Fn. 1), S. 318.

haben vielfach einen grossen Einfluss auf die abschliessende Qualifikation der Überschuldungssituation. Ein Verwaltungsrat sollte sich dabei nicht auf die Angaben der eigenen IT-Abteilung verlassen. Vielmehr sind externe Bewertungen vornehmen und der Revisionsstelle vorlegen zu lassen.

Die Benachrichtigung des Richters wegen Überschuldung kann nicht nur in physischer Form sondern gemäss Art. 130 ZPO auch in elektronischer Form erfolgen. Dabei muss das Dokument, welches den Antrag auf Konkurseröffnung wegen Überschuldung und Unmöglichkeit einer Sanierung enthält, mit einer anerkannten elektronischen Signatur des Absenders versehen sein. Bei elektronischer Übermittlung kann das Gericht zudem verlangen, dass die Eingabe und die Beilagen in Papierform nachgereicht werden. Auch in prozessualer Hinsicht hat das digitale Zeitalter vieles verändert.

III. Verwaltungsrat und Datenschutz

1. Datenschutzrechtliche Pflichten des Verwaltungsrates

Im Aktienrecht besteht eine umfassende Kompetenzvermutung zugunsten des Verwaltungsrates, woraus ein umfangreicher Aufgabenkatalog resultiert. Art. 716 Abs. 1 OR legt fest, dass der Verwaltungsrat in allen Angelegenheiten Beschluss fassen kann, die nicht durch Gesetz oder Statuten einem anderen Organ zugeteilt sind. Der Verwaltungsrat ist damit das Exekutivorgan der Gesellschaft schlechthin.²³ Dieses zentrale Zuständigkeitsprinzip ist aus systematischen und sachlichen Gründen zwingend. Die Führung der Geschäfte ist den Kapitalgebern entzogen und einem klar geregelten Zwischenglied, dem Verwaltungsrat, anvertraut. Je nach konkreter Situation der Aktiengesellschaft kann diese umfassende Kompetenz beim Verwaltungsrat belassen und ihm dadurch ein maximaler Handlungsspielraum eingeräumt werden.²⁴ Gemäss Art. 716b OR kann die Geschäftsführung im Rahmen der Bestimmungen eines Organisationsreglements ganz oder zum Teil an einzelne Mitglieder des Verwaltungsrates oder an Dritte übertragen werden.

Aus den Pflichten des Verwaltungsrates kann abgeleitet werden, dass jeder Verwaltungsrat auch im Bereich Datenschutz die oberste Verantwortung trägt. Der Verwaltungsrat hat die unübertragbare und unentziehbare Aufgabe zur Oberleitung der Gesellschaft.²⁵ Primär ist damit die Pflicht des Verwaltungsrates verbunden, die Ge-

²³ BÖCKLI (Fn. 17), § 13 Rz. 287.

²⁴ Eine Liste von Pflichten, die nicht in Art. 716a OR aufgeführt sind, findet sich bei JÖRG FLORIAN S., Das Mitglied des Verwaltungsrates als Superman? – Pflichten und Tipps, in: Florian S. Jörg/Oliver Arter (Hrsg.), Entwicklungen im Gesellschaftsrecht VI, Bern 2011, S. 305 f.

²⁵ FORSTMOSER/MEIER-HAYOZ/NOBEL (Fn. 10), § 30 Rz. 31 ff.; BÖCKLI (Fn. 17), § 13 Rz. 306.

sellschaftsziele mit den Gesellschaftsmitteln in Einklang zu bringen und die Organisation der Gesellschaft entsprechend zu gestalten.²⁶

Zu dieser Oberleitung gehört es auch, die Informationssicherheit zu garantieren. Hochsensible Daten bspw. zur Unternehmensentwicklung oder Strategie sind sowohl gegen externen als auch gegen internen unbefugten Zugriff zu schützen. Damit ist klar, dass den Verwaltungsrat die Pflicht trifft, sich mit der IT-Situation der Gesellschaft auseinanderzusetzen. Des Weiteren ist der Verwaltungsrat verpflichtet, für die dauernde Erhaltung des Gleichgewichts zwischen Zielen und Mitteln zu sorgen sowie einzugreifen, wenn die Dinge aus dem Ruder laufen. Allerdings können strategische Ziele in der Regel nur erreicht werden, wenn beim Einsatz der Mittel ein kalkuliertes Risiko in Kauf genommen wird.²⁷ Derartige Risiken dürfen jedoch weder die Existenz des Unternehmens noch die Integrität von Menschen gefährden. In punkto Sicherheit hat das Bundesgericht in mehreren Fällen klargestellt, dass dies Chefsache sei.²⁸ Das bedeutet für den Verwaltungsrat konkret, dass es nicht genügt, lediglich einen Sicherheitsbeauftragten zu bestellen und dann alle Hinweise auf Gefahren zu ignorieren. Vielmehr ist die Gefahrenlage zu beobachten und der Sicherheitsbeauftragte zu überwachen. Gegebenenfalls ist der Sicherheitsbeauftragte anzuweisen, drohende Gefahren zu beseitigen. Analoges muss auch für den Bereich Datenschutz und die damit verbundenen Risiken gelten.

Mit der Oberleitung bzw. mit dem entsprechenden Weisungsrecht eng verbunden ist die Pflicht des Verwaltungsrates, im Falle einer Delegation der Geschäftsführung die Mitglieder der Geschäftsleitung zu ernennen und zu überwachen. Diese Pflicht zur Oberaufsicht kommt ihm gemäss Art. 716a Ziff. 5 OR zu. Diese Oberaufsicht ist so auszugestalten, dass eine optimale Unternehmensüberwachung möglich wird.²⁹ Die Beaufsichtigung beinhaltet dabei sowohl die im Gesetz umschriebene Überwachung im Hinblick auf die Befolgung von Gesetz, Statuten, Reglementen und Weisungen als auch die Hinterfragung von Geschäftsführungshandlungen nach technischen, sozialen und betriebswirtschaftlichen Kriterien. Zu den Gesetzen, welche von der Geschäftsleitung eingehalten werden müssen, zählt auch das Datenschutzgesetz. Ebenso wie beim Thema Sicherheit ist daher klar, dass es bezüglich Datenschutz nicht genügen kann, lediglich einen Datenschutzbeauftragten zu bestellen und dann alle Hinweise auf Verletzungen des Datenschutzgesetzes zu ignorieren. Vielmehr hat der Verwaltungsrat den Datenschutzbeauftragten zu überwachen und gegebenenfalls

²⁶ MÜLLER/LIPP/PLÜSS (Fn. 1), S. 157.

²⁷ KRNETA GEORG, Praxiskommentar Verwaltungsrat – Ein Handbuch für Verwaltungsräte, 2. Aufl. Bern 2005, Rz. 1191.

²⁸ Nachweis in MÜLLER/LIPP/PLÜSS (Fn. 1), S. 163 f.

²⁹ BÖCKLI (Fn. 17), § 13 Rz. 356a.

anzuweisen, drohende Verletzungen zu beseitigen. Es kann damit festgehalten werden, dass der Verwaltungsrat der oberste Datenschutzler im Unternehmen ist.

2. Problematische Bereiche

a) Übersicht

In einem digitalen Zeitalter sind die Herausforderungen punkto Datenschutz im Unternehmen sehr vielfältig. Aktuelle Trends, wie bspw. biometrische Zugangskontrollen, telematische Systeme zur Überwachung und zum Managen des Fuhrparks oder ganz allgemein die grenzüberschreitende Datenspeicherung werfen Fragen zur Kompatibilität u.a. mit datenschutzrechtlichen Bestimmungen auf. Im Folgenden sollen drei konkrete Beispiele kurz dargestellt werden.

b) Biometrie

Biometrie beschreibt die Identitätsfeststellung einer Person durch ihre biologischen bzw. psychologischen, physikalischen, physiologischen oder verhaltenstypischen Merkmale.³⁰ Mit Hilfe von biometrischen Daten, also Angaben aus biometrischen Merkmalen in Form von Mustern oder Rohdaten, könnten aus rein technischer Optik diverse Vorgänge in einem Unternehmen gesteuert werden. Bspw. wäre es möglich, Fingerabdrücke für eine automatische Zeiterfassung einzusetzen oder die Kasse mittels Venenstrukturanalyse oder Handgeometrie zu entsperren. Bekannt sind auch Netzhautscans, Handabdrücke, Stimmerkennung, Ohrengometrie oder die Gesichtserkennung. Alle diese biometrischen Merkmale könnten durch biometrische Verfahren zur Zugangskontrolle logischer oder physischer Art benutzt werden. Es stellt sich dabei jedoch die Frage, ob diese Verfahren, bspw. die Zeiterfassung durch Fingerabdrücke, datenschutzrechtlich zulässig sind.

Bei Fingerabdrücken und daraus extrahierten Minuzien³¹ handelt es sich um statische biometrische Daten. Sie sind zeitlich unveränderliche und unverwechselbare Wesensmerkmale einer Person, die sich andere Personen nicht aneignen können.³² Ohne Verbindung zur Identität stellen die biometrischen Elemente keine Personendaten dar; mit Verbindung zur Identität bilden die Fingerabdrücke hingegen (besonders) schützenswerte Personendaten im Sinne des Datenschutzgesetzes, da sich daraus die

³⁰ Vgl. dazu MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, Rz. 2241; JAIN ANIL K./ROSS ARUN A., Introduction to Biometrics, in: Anil K. Jain/Patrick Flynn J./Arun A. Ross (Hrsg.), Handbook of Biometrics, New York 2008, S. 1.

³¹ Minuzien sind bestimmte Merkmale des Fingerabdrucks, wie Punkte mit einer Gabelung oder einem Linienende und Rillen auf der Fingeroberfläche.

³² EDÖB, Anwesenheitskontrollen mit Hilfe von Fingerabdrücken.

Rassenzugehörigkeit rekonstruieren lässt (was für Minuzien alleine nicht der Fall ist),³³ was zur Anwendbarkeit des Datenschutzgesetzes führt.

Es sind im Folgenden zwei Fälle zu unterscheiden.³⁴ Im ersten Fall wird eine Erfassung der Fingerabdrücke nicht mit Personendaten verknüpft. Dies kann dadurch ermöglicht werden, dass zunächst ein digitales Bild des Fingerabdrucks erstellt wird, um die Minuzien herauszufiltern. Im Folgenden reicht es für die Autorisierung bspw. eines Zugangs aus, wenn das System die Minuzien des Fingers später mit den Referenzminuzien vergleicht. Dabei bleibt der Arbeitnehmer aber anonym. Dieses System ist daher für den hier untersuchten Zweck bspw. für die Arbeitszeiterfassung ungeeignet, denn die Arbeitszeit soll ja einer bestimmten Person gutgeschrieben werden. Im zweiten Fall werden Personendaten mit den biometrischen Daten verknüpft, d.h. ein Fingerabdruck wird einer bestimmten Person zugewiesen, womit diese Daten zu schützenswerten Personendaten im Sinne von Art. 3 Bst. c Ziff. 2 DSG werden. Der Verwaltungsrat muss sich deshalb im heutigen digitalen Zeitalter der nachstehenden Problematik im Zusammenhang mit dem Datenschutz bewusst sein.

Das Erfassen von verknüpften biometrischen Daten resp. deren Verwendung fällt unter den Begriff der Datenbearbeitung gemäss Art. 3 Bst. e DSG und damit unter Art. 328b OR. Art. 328b OR beschränkt die zulässige Datenbearbeitung im Arbeitsverhältnis auf Fälle mit Arbeitsplatzbezug, resp. auf Datenbearbeitungen, welche zur Durchführung des Arbeitsvertrages erforderlich sind. Es ist im Rahmen des Arbeitsverhältnisses durchaus notwendig, dass der Arbeitgeber persönliche Daten der Mitarbeiter bearbeitet.³⁵ Die Datenbearbeitung muss darüber hinaus auch noch verhältnismässig im Sinne von Art. 4 Abs. 2 DSG sein; d.h. es ist das mildeste Mittel anzuwenden, mit dem der für die Durchführung des Arbeitsverhältnisses notwendige Zweck erreicht werden kann.

Aus arbeitsrechtlicher Sicht ist das zentrale Speichern von verknüpften biometrischen Daten problematisch, denn in den meisten Fällen ist dies für die Durchführung des Arbeitsverhältnisses nicht zwingend notwendig. Ginge man davon aus, die Erfassung von biometrischen Daten sei zur Durchführung des Arbeitsverhältnisses notwendig, so ist zu prüfen, ob nicht ein milderer Mittel den gleichen Erfolg erzielt. Das Bundesverwaltungsgericht hat entschieden, dass es mildere Mittel als eine zentrale Speicherung biometrischer Daten gebe und die zentrale Speicherung daher unverhältnismässig, persönlichkeitsverletzend und nicht datenschutzkonform sei.³⁶ Das Bundesverwal-

³³ Vgl. Art. 3 Bst. c Ziff. 2 DSG.

³⁴ Vgl. zum Ganzen: EDÖB, Leitfaden zu biometrischen Erkennungssystemen, Bern 2009.

³⁵ STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag, 7. Aufl. Zürich/Basel/Genf 2012, Art. 328b OR Rz. 6.

³⁶ BVGE 2009/44 E. 6.

tungsgericht führte aus, dass diese Daten für den Vergleich auch auf einer Smartcard³⁷ gespeichert werden können, welche im Besitz des Betroffenen bleibt. Dadurch sei immer noch der höhere Sicherheitsstandard erreicht als bei einer blossen Magnetkarte, denn dann muss Smartcard und Fingerabdruck übereinstimmen, um Zugang zu erlangen. Die Lösung über die Smartcard ist auch für eine Zeiterfassung denkbar. Diese ist jedoch nur dann zulässig, wenn tatsächlich eine erhöhte Sicherheitsstufe bezweckt wird. Wird lediglich eine einfache Registrierung bezweckt, würde der Einsatz einer Magnetkarte denselben Zweck erfüllen und wäre eindeutig das mildere Mittel. Die Lösung mittels Smartcard hätte bei der Zeiterfassung neben der erhöhten Sicherheit aber keine vereinfachende Wirkung, da der Arbeitnehmer immer noch eine zusätzliche Karte mitführen muss. Will ein Verwaltungsrat ein Zeiterfassungssystem mittels biometrischer Daten einführen, sollten zunächst die Arbeitnehmer konsultiert werden. Danach muss eine Einwilligung der betroffenen Arbeitnehmer eingeholt werden (Art. 4 Abs. 5 DSG). Des Weiteren sind besondere Massnahmen zum Schutz dieser Daten zu ergreifen, wie z.B. die Chiffrierung der bearbeiteten Daten. Alle Bearbeitungsschritte – das Speichern, der Vergleich und die Übermittlung von Personendaten – müssen geschützt werden. Der Zweck der Datenbearbeitung muss den betroffenen Personen mitgeteilt werden. Mindestens in einer Übergangsphase führt die gesetzlich vorgeschriebene ausdrückliche Einwilligung dazu, dass zwei Zeiterfassungssysteme parallel eingesetzt werden müssen, eines für alle Mitarbeitenden die ihre Einwilligung abgegeben haben und eines für den Rest der Mitarbeitenden.

Aus arbeits- und datenschutzrechtlicher Sicht gibt es also Möglichkeiten, die Zeiterfassung aufgrund biometrischer Daten vorzunehmen. Ebenso ist jedoch ersichtlich, dass im Bereich Biometrie nicht alles erlaubt ist, was technisch möglich ist. Der Verwaltungsrat hat in seiner Funktion als oberster Datenschützer im Betrieb zu verhindern, dass Systeme eingesetzt werden, welche die Persönlichkeit seiner Mitarbeitenden verletzen. Soll ein System eingeführt werden, das aus arbeits- oder datenschutzrechtlicher Sicht zu einer Persönlichkeitsverletzung der Mitarbeitenden führt, hat er zu intervenieren und nötigenfalls entsprechende Weisungen an die Geschäftsführung zu erteilen. Ein Verwaltungsrat wird sich in aller Regel nicht damit entlasten können, dass er angibt, von dieser Einführung nichts gewusst zu haben, denn spätestens bei der Genehmigung des Budgets wird er Kenntnis von der Einführung dieses Systems erlangen. Einem Verwaltungsrat ist damit zu empfehlen, bei entsprechenden Hinweisen genauere Informationen zu verlangen und nötigenfalls zu intervenieren.

³⁷ Dabei handelt es sich um eine Speicherkarte, auf der biometrische Referenz-Templates (Repräsentation eines biometrischen Rohdatums) gespeichert und mit erfassten biometrischen Proben verglichen werden können.

c) Grenzüberschreitende Datenspeicherung

Die Digitalisierung hat bereits seit längerem auch im Rahmen der Archivierung eingesetzt. Immer mehr werden Dokumente nicht mehr ausschliesslich in Papierform, sondern auch elektronisch gespeichert und archiviert. Obwohl es sich dabei nicht um ein neues Thema handelt, tauchen immer wieder Fragen im Zusammenhang mit der Datenspeicherung auf, welche der Aufmerksamkeit des Verwaltungsrates bedürfen. Oft entscheiden im Bereich Datenschutz bereits kleine Änderungen an Infrastruktur oder Prozessablauf über die Zulässigkeit oder Unzulässigkeit einer Datenbearbeitung. Zur Verdeutlichung soll dabei die Datenspeicherung im Ausland dienen.

Eine schweizerische Aktiengesellschaft, welche Tochter eines internationalen Konzerns ist, möchte ihre Personendaten zukünftig auf Servern in Deutschland speichern. Der Zugriff auf die Personendaten soll dabei auf Mitarbeitende der Schweizer Tochter beschränkt bleiben. Aus Sicht des schweizerischen Datenschutzrechts stellen sich dabei mehrere Fragen. Art. 6 DSG regelt die Datenübermittlung ins Ausland. Demnach dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.³⁸ Zu klären gilt es damit, ob die Speicherung der Daten auf einem Server im Ausland als «Bekanntgabe» im Sinne von Art. 3 Bst. f DSG und ob Deutschland als Land mit genügend hohem Datenschutz gemäss Art. 6 Abs. 1 DSG gilt.

Der Begriff «Bekanntgeben» in Art. 6 Abs. 1 DSG entspricht jenem von Art. 3 Bst. f DSG und wird dort definiert. Das Gesetz definiert das «Bekanntgeben» als das Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen. Die Datenbekanntgabe stellt datenschutzrechtlich einen der sensibelsten Bearbeitungsschritte dar, nicht zuletzt, da sie auf vielfältige Art und Weise erfolgen kann.³⁹ Namentlich gelten jede aktive Weitergabe und jedes passive Zugänglichmachen, die es einem Dritten ermöglichen, vom Inhalt personenbezogener Informationen Kenntnis zu nehmen, als Bekanntgabe.⁴⁰ Mögliche Auslöser einer Übermittlung von Personendaten ins Ausland können sein⁴¹:

- die Zentralisierung einer bestimmten Datenbearbeitung
- das Outsourcing von Datenbearbeitungen

³⁸ Art. 6 Abs. 1 DSG.

³⁹ BLECHTA GABOR P., in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar, Datenschutzgesetz – Öffentlichkeitsgesetz, 3. Aufl. Basel 2014, Art. 3 DSG Rz. 76.

⁴⁰ BLECHTA (Fn. 39), Art. 3 DSG Rz. 77.

⁴¹ Vgl. dazu auch EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland, Bern 2014, S. 4.

- die Übernahme durch ein ausländisches Unternehmen

Insbesondere im Fall eines sogenannten «Abrufverfahrens» ist eine genaue Analyse erforderlich, da es einen erheblichen Eingriff in die Grundrechte der betroffenen Personen darstellt. Beim Abrufverfahren handelt es sich um ein automatisiertes Verfahren, welches dem Datenempfänger ermöglicht, Daten aus einem Informationsbestand selber zu beschaffen.⁴² Durch dieses Verfahren wird die Kontrolle der Rechtmässigkeit einer Bekanntgabe von Personendaten im Einzelfall erheblich erschwert. Ein solches Verfahren ist daher als «Gefährdung der Persönlichkeit» zu qualifizieren.⁴³ Gemäss dem Muster-Sachverhalt ist ein Zugreifen auf die Daten durch Dritte jedoch nicht möglich. Demnach handelt es sich bei der reinen Speicherung von Daten im Ausland noch nicht um ein «Bekanntgeben» im Sinne von Art. 3 Bst. f und Art. 6 Abs. 1 DSG. Im Falle eines Outsourcings von Datenbearbeitungen, bspw. in kostenarme Länder, ist die Sachlage anders zu beurteilen.

Das schweizerische Datenschutzgesetz gewährleistet den Schutz der Privatsphäre für Datenbearbeitungen, die von Personen in der Schweiz vorgenommen werden. Wenn aber Daten ins Ausland übermittelt werden sollen, muss sichergestellt sein, dass diese Daten dort angemessen geschützt sind. Obwohl die Speicherung nicht als Bekanntgabe qualifiziert werden kann, unterstehen die Server dem Recht des Landes, in dem sie stehen. Es muss damit sichergestellt werden, dass dieses Land einen angemessenen Schutz der Daten gewährleistet.⁴⁴ Denn Art. 6 Abs. 1 DSG verbietet die Bekanntgabe von Personendaten ins Ausland, sofern eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Würde ein angemessener Schutz fehlen, wäre es möglich, dass das «Standortland» eine Datenherausgabe verfügt, welche nach dem Gesetz des entsprechenden Landes zwar zulässig, nach Schweizer Recht jedoch unzulässig wäre. Dies wäre dann eine Datenbekanntgabe im Sinne von Art. 3 und 6 DSG. Ob in einem Land ein angemessener Schutz vorhanden ist, ist auf der «Staatenliste» des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) ersichtlich. Deutschland wird auf dieser Liste geführt.

Im Übrigen gilt, dass die übermittelten Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.⁴⁵ Darum empfiehlt es sich, je nach Klassifizierung der Datenkategorien besondere Schutzmassnahmen zu ergreifen. Gemäss EDÖB muss garantiert sein, dass zu jeder Zeit der unberechtigte Zugang zur Infrastruktur und zu den Datenträgern

⁴² BLECHTA (Fn. 39), Art. 3 DSG Rz. 77.

⁴³ So zumindest die Eidgenössische Datenschutz- und Öffentlichkeitskommission im Entscheid VPB 68.92 E. 3.b.

⁴⁴ EDÖB (Fn. 34), Erläuterungen zur Übermittlung von Personendaten ins Ausland, S. 5.

⁴⁵ Art. 7 DSG.

unmöglich ist. Ebenso muss der Zugriff Unberechtigter auf die Personendaten, während deren Lagerung und Transport ausgeschlossen sein, indem die Daten verschlüsselt werden. Die Verschlüsselung hat nach dem aktuellen Stand der Technik zu erfolgen. Dies gilt sowohl für die Daten als auch für die Datenschutzerklärungen. Die Identifikation der gemäss Erklärungen Empfangsberechtigten muss eindeutig gewährleistet sein. Die Identifikation hat nach den neusten technischen Stand zu erfolgen. Damit jederzeit die Verarbeitung der Daten nachvollziehbar ist, muss sie protokolliert werden.⁴⁶

Solange die Gesellschaft in der Schweiz sicherstellt, dass die übermittelten Personendaten gegen unbefugtes Bearbeiten geschützt werden und auch tatsächlich keine «Bekanntgabe» im Sinne von Art. 3 Bst. f DSG ins Ausland erfolgt, ist die Speicherung von Personendaten in Deutschland zulässig, solange die übrigen datenschutzrechtlichen Bestimmungen und Grundsätze ebenfalls eingehalten werden. Dieses Beispiel zeigt deutlich, dass Verwaltungsräte gut daran tun, Vorgänge und Prozesse genau zu analysieren und sich über die Details zu informieren. Denn bereits die Änderung der Zugriffsberechtigung kann zu einer grundlegend anderen Beurteilung der Sachlage mit entsprechend unterschiedlichen Rechtsfolgen führen. Werden aufgrund dieser unbemerkten Änderung bspw. Meldepflichten nicht wahrgenommen,⁴⁷ steht der Verwaltungsrat unter Umständen in der Verantwortung.

3. Folgen einer datenschutzrechtlichen Verletzung

Art. 15 DSG regelt die Rechtsansprüche, die einer mit unzulässiger Datenbearbeitung konfrontierten Person offen stehen. Klagen zum Schutz der Persönlichkeit richten sich nach den Art. 28, 28a sowie 28/ ZGB.⁴⁸ Die verletzte Person kann insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden. Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann verlangt werden, dass bei den Daten ein entsprechender Vermerk angebracht wird. Zudem kann verlangt werden, dass die Berichtigung, die Vernichtung, die Sperre, namentlich die Sperre der Bekanntgabe an Dritte, der Vermerk über die Bestreitung oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

⁴⁶ ED ÖB, Die Bekanntgabe von Personaldaten ins Ausland, Tätigkeitsbericht 2001/2002, Juli 2002.

⁴⁷ Vgl. bspw. Art. 6 Abs. 3 DSG.

⁴⁸ Art. 15 Abs. 1 DSG.

Den Verwaltungsrat trifft bei einer Verletzung seiner datenschutzrechtlichen Pflichten zudem unter Umständen eine persönliche Verantwortlichkeit.⁴⁹ Zum Verantwortlichkeitsrecht hat sich in neuerer Zeit eine kaum mehr überblickbare Literatur und Rechtsprechung ergeben.⁵⁰ Doch neben der zivilrechtlichen Verantwortlichkeit wird häufig übersehen, dass die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten sowie der beruflichen Schweigepflicht zu strafrechtlichen Sanktionen führen kann. Die notwendigen Grundlagen finden sich in den Art. 34 und 35 DSG. Obwohl die genannten Artikel zum Nebenstrafrecht zählen, handelt es sich dennoch um Strafrecht, womit auch der Allgemeine Teil des Strafgesetzbuches zumindest subsidiär Anwendung findet.⁵¹ Die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten sowie der beruflichen Schweigepflicht wird mit Busse bestraft. Vorausgesetzt für die Anwendung von Art. 34 DSG sind eine (private) Datensammlung und die Verletzung bestimmter damit zusammenhängender Pflichten, insbesondere durch den, der über Zweck und Inhalt der Datensammlung entscheidet, der also (Mit-)Inhaber der Datensammlung ist.⁵² Täter kann also nur sein, wen eine der in Art. 34 DSG genannten Pflichten trifft. Es handelt sich um ein echtes Sonderdelikt. Der Pflichtige ist jedoch nicht nur für seine eigenhändig falsch erteilte Auskunft verantwortlich, sondern auch für die bspw. von einem Angestellten gemäss seiner Weisung falsch erteilten Auskunft.⁵³ Ist eine juristische Person oder Gesellschaft pflichtig, sind grundsätzlich die natürlichen Personen verantwortlich, die effektiv für das Unternehmen handeln und den Tatbestand schuldhaft erfüllen.⁵⁴ Nicht anwendbar sind die Bestimmungen über die Verantwortlichkeit des Unternehmens, da es sich bei den Delikten gemäss Art. 103 StGB um Übertretungen handelt.⁵⁵ Dies gilt auch für Art. 35 DSG.

Aus diesen Ausführungen ist deutlich ersichtlich, dass sich der Verwaltungsrat mit der Thematik Datenschutz in seinem Unternehmen auseinandersetzen muss. Das Nichtwissen über eine Verletzung des Datenschutzes könnte dem Verwaltungsrat u.U. als Sorgfaltspflichtverletzung ausgelegt werden.⁵⁶ Aber auch strafrechtlich kann der Verwaltungsrat persönlich zur Verantwortung gezogen werden. Jeder Verwaltungsrat sollte sich daher seiner Pflicht als oberster Datenschützer im Unternehmen stets bewusst sein.

⁴⁹ Art. 752 ff. OR.

⁵⁰ Vgl. Nachweis bei MÜLLER (Fn. 8), S. 975 f.

⁵¹ NIGGLI MARCEL ALEXANDER/MAEDER STEFAN, in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar, Datenschutzgesetz – Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, Vorbemerkungen Art. 34 und 35 DSG Rz. 13.

⁵² Art. 3 Bst. i DSG; NIGGLI/MAEDER (Fn. 51), Art. 34 DSG Rz. 17.

⁵³ NIGGLI/MAEDER (Fn. 51), Art. 34 DSG Rz. 18.

⁵⁴ BGE 110 IV 17; 106 IV 22; 105 IV 175; 97 IV 292; NIGGLI/MAEDER (Fn. 51), Art. 34 DSG Rz. 19.

⁵⁵ Vgl. dazu Art. 102 StGB.

⁵⁶ Vgl. Art. 716, 716a, 716b, 717 und 754 OR.

IV. Zusammenfassung und Empfehlungen

Verwaltungsräte haben im digitalen Zeitalter eine zusätzliche Aufgabe: die Information Governance. Nicht mehr die Speicherung von Daten ist das Problem, sondern der Umgang mit diesen Daten. Auf strategischer Führungsebene ist festzulegen, welche Verfahren, Organisationen und Technologien benötigt werden, um Daten während ihres gesamten Lebenszyklus⁵⁷ in Übereinstimmung (Compliance) mit externen und internen Regulierungen aktiv zu bewirtschaften. In diesem Sinne umfasst Information Governance auch Teilbereiche des Information Managements (MIS) und des Risk Managements.

Neue Technologien, wie insbesondere Internet-Kaufplattformen und Social Media, zwingen Verwaltungsräte, sich mit der digitalen Transformation auseinanderzusetzen. Daten sind die Währung des Informationszeitalters.⁵⁸ Durch das Erheben, Aufbewahren und Auswerten grosser Mengen von Daten (sog. Big Data) können datenbasierte Entscheidungsgrundlagen geschaffen werden, mit deren Hilfe Unternehmen effizienter werden. Doch nicht nur neue Technologien, auch verändertes Konsumverhalten, neue Regulierungen im Bereich des Datenschutzes und das gesteigerte Kostendenken sind die Treiber der Digitalisierung.

Die laufende Überprüfung und Anpassung der Unternehmensstrategie ist im digitalen Zeitalter noch wichtiger geworden. Neue spontane Geschäftsentwicklungen und daraus resultierende Konkurrenz (wie Uber als Beispiel für die Teilung von Investitionsgütern) sind genauso eine Herausforderung für Verwaltungsräte wie die Möglichkeit der «economy on demand». Um Währungsproblemen zu begegnen, werden von den Unternehmen so wenig Mitarbeiter wie möglich angestellt und dafür ausgelagerte Dienstleistungen (auch im IT-Bereich) aus dem Ausland bezogen.

Bei allen strategischen Vorteilen, welche das digitale Zeitalter mit sich bringt, dürfen Verwaltungsräte aber die damit verbundenen Risiken und Gefahren nicht ausser Acht lassen. Nicht mehr physische Sicherheitsüberlegungen sondern virtueller Schutz gegen Attacks von Innen und Aussen sind gefragt. Dies führt zu wesentlichen Änderungen in der IT-Organisation. Nicht mehr der IT-Chef ist Verantwortlicher der Daten, sondern der entsprechende Geschäftsbereichsleiter.

Damit hat der Verwaltungsrat im Bereich Information Governance letztlich folgende Aufgaben zu lösen:

⁵⁷ Dazu gehören das Erfassen, das Klassieren, das Speichern, das Nutzen und das Löschen von Daten.

⁵⁸ Erläuternder Bericht Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG) vom 26. März 2014, S. 9.

- Strategische Festlegung der IT-Ziele und der IT-Mittel
- Weitsichtige Organisation des IT-Bereiches und entsprechende Teamentwicklung
- Umfassende Kommunikation zu IT-Fragen gegen Innen und Aussen
- Laufende Kontrolle von IT-Compliance und IT-Sicherheit