Der europäische Datenschutz als wertschöpfender Faktor betrieblicher Compliance vor dem Hintergrund aktueller Entwicklungen

Bachelorarbeit

Ausgeführt zum Zweck der Erlangung des akademischen Grades
Bachelor der Rechts- und Wirtschaftswissenschaften (LLB.oec)

am Bachelorstudiengang Recht und Wirtschaft
an der Paris Lodron Universität Salzburg

von:
Thomas Pickl
0614136

Betreuer: Prof. Dr. Christoph Schließmann

Salzburg, 8.7.2015

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Thema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der von dem Begutachter beurteilten Arbeit überein.

....

Salzburg, 8.7.2015 Unterschrift

Gender-Klausel

Die weibliche Form ist in dieser Bachelorarbeit der männlichen Form gleichgestellt; lediglich aus Gründen der leichteren Lesbarkeit wurde die männliche Form gewählt.

Inhaltsverzeichnis

1 Einleitung

Wir schreiben das Jahr 1989. Genf, Schweiz. Der britischer Wissenschaftler Tim Berners-Lee erfindet am CERN das World Wide Web. Das „Web“ soll Wissenschatlern den automatischen Informationsaustausch zwischen Universitäten und Instituten rund um den Erdball ermöglichen.[1]

Ein Sprung ins Jahr 2015. Das Web hat sich längst seinen Weg in die Privathaushalte und Unternehmen gebahnt. Über das Internet werden Dienste wie das Web, E-Mail oder FTP genutzt, Daten ausgetauscht und Informationen beschafft. Fotos werden auf Instagram hochgeladen, Beiträge auf Facebook kommentiert und die neuesten Infos über Twitter verbreitet. Der Mensch hat sich eine virtuelle Präsenz geschaffen und wurde zu einem gläsernen Objekt voller Informationen und Daten. Forscher der Cambridge und der Stanford Universität haben in einer Studie festgestellt, dass ab einer gewissen Anzahl von „Likes“ auf Facebook der Computer mehr über die Persönlichkeit eines Menschen sagen kann als enge Freunde und Familienmitglieder.[2] Das Informationszeitalter ist längst angebrochen. Unternehmen wissen um den Wert von Daten und versuchen diesen zu nutzen, um Wettbewerbsvorteile zu erzielen und Profit zu schlagen. Die Grenzen zwischen erlaubten Umgang mit Informationen und verbotenem Zugriff auf persönliche Daten werden ausgelotet und Enthüllungsskandale à la Edward Snowden steigern das Bewusstsein der Menschen um die Wichtigkeit und den Wert ihrer persönlichen Daten und erwecken den Wunsch, ebendiese bestmöglich geschützt zu sehen.

---

[1] Vgl. CERN: The birth of Web, http://home.web.cern.ch/topics/birth-web, abgefragt am 6.7.2015

[2] Vgl. Youyou, W./Kosinski, M./Stillwell, D., Studie: Computer-based personality judgements are more accurate than those made by humans, http://www.pnas.org/content/112/4/1036.full, abgefragt am 6.7.2015

Der Datenschutz ist keine neue, durch das Internet ausgelöste Thematik, aber wurde durch dessen Siegeszug auf ein völlig neues Level gehoben. Durch den gesellschaftlichen Wandel im Umgang mit Daten stellt sich unweigerlich die Frage, ob die gesetzlichen Regelungen in Bezug auf den Schutz personenbezogener Daten noch den Anforderungen entsprechen. In Europa fußt der Datenschutz noch auf einer Regelung, die aus den Anfängen des Internetzeitalters stammt und daher antiquiert und unzulänglich erscheint. Die aktuellen Entwicklungen in der EU zeigen Bemühungen dieses Problem zu lösen und eine Regelung zu schaffen, die sowohl Privatpersonen als auch Unternehmen zum Vorteil gereicht. Gerade für Letztere stellt sich der Datenschutz - je strenger die Bestimmungen ausfallen - als lästige Pflicht und als vermeintlicher Hemmschuh für wirtschaftlich erfolgreiches Handeln dar. Gesetzliche Bestimmungen müssen in Form von betrieblicher Compliance eingehalten werden, Kosten fallen an und ganz allgemein haftet dem Datenschutz aus Unternehmenssicht ein handlungsbeschränkender und profithemmender Ruf an.

In dieser Arbeit soll vor diesem Hintergrund die Frage behandelt werden, ob der europäische Datenschutz dementgegen auch positive und gewinnbringende Aspekte entfalten und für Unternehmen einen nutzenstiftenden Faktor für die Wertschöpfung darstellen kann. Zu diesem Zwecke wird zunächst der gesetzliche Rahmen abgesteckt und die Rolle des Datenschutzes als Bestandteil betrieblicher Compliance im europäischen Raum definiert. Dies geschieht sowohl durch Betrachtung der aktuellen Gesetzeslage als auch durch einen Einblick in die gesetzliche Entwicklung innerhalb der EU, um die unternehmerische Sicht auf den Datenschutz und seine Entwicklung zu veranschaulichen. In weiterer Folge wird die Rolle des Datenschutzes für die Wertschöpfung innerhalb dieses Rahmens analysiert. Dabei werden sowohl allgemeine wertschöpfende Faktoren des Datenschutzes als auch spezielle Eigenheiten - die sich durch den europäischen Datenschutz und dessen Entwicklung ergeben - berücksichtigt.

Ziel dieser Arbeit ist es, einen Überblick über die Rolle des Datenschutzes als Bestandteil betrieblicher Compliance in Europa darzulegen und dabei sowohl die aktuelle als auch die zukünftige Situation miteinzubeziehen. Innerhalb dieses Spannungsfeldes soll die Frage beantwortet werden, ob und in welcher Form der Datenschutz in Unternehmen einen Nutzen für die Wertschöpfung darstellen kann

und wie sich diese Möglichkeit vor dem Hintergrund der aktuellen Entwicklungen in Europa ausprägt.

2 Der europäische Datenschutz als Bestandteil betrieblicher Compliance

2.1 Die Datenschutz-Compliance

Die Unternehmensleitung hat die Aufgabe ihre unternehmerischen Tätigkeiten nach den gesetzlichen Bestimmungen durchzuführen und zu überwachen, dass jede Handlung im gesamten Unternehmen den Gesetzen entspricht. Diese Einhaltung des mit staatlichen Sanktionen bewehrten Rechts kann als Mindestanforderung an die Leitungsaufgabe „Compliance“ gesehen werden. Dabei erstreckt sich der zu beachtende gesetzliche Rahmen auf unterschiedliche Bereiche wie das Anti-Korruptionsrecht, das Wettbewerbsrecht, das Außenwirtschaftsrecht, das Umweltschutzrecht oder eben auch das Datenschutzrecht. Compliance stellt Unternehmen vor eine herausfordernde Aufgabe, die sich umso komplexer gestaltet, je internationaler das Unternehmen auftritt und je unterschiedlicher die Produktions- oder Vertriebszweige sind. Die Verantwortung für die Compliance liegt - ungeachtet einer möglichen Delegierung an Fachabteilungen - ausschließlich bei der Unternehmensleitung. Diese muss zunächst eine Risikoabschätzung vornehmen, welche sowohl die unternehmensinternen Geschäftspraktiken als auch die geschäftlichen Beziehungen zu externen Geschäftspartnern miteinbeziehen muss. Danach ist ein Compliance Programm aufzusetzen und eine adäquate Compliance Organisation zu installieren, was sich von Unternehmen zu Unternehmen äußerst unterschiedlich darstellen kann. Dieses Compliance Management System (CMS) sollte stets systematisch aufgebaut sein und durch seine Maßnahmen die drei Grundfunktionen einer funktionierenden Compliance berücksichtigen: Prävention, Aufdeckung und Reaktion. Außerdem muss das Compliance Programm in die Geschäftsprozesse integriert werden und zwar nicht durch bloße Übersendung eines

Verhaltenskodex an die Mitarbeiter, sondern durch praxisnahe und verständnisschaffende Implementierung. Der Fokus liegt dabei auf der Verhinderung von systematischen Fehlverstößen und dem Früherkennen von Warnzeichen, um erforderliche Gegenmaßnahmen einleiten zu können.[3] In diesem Zusammenhang können die Begriffe Compliance, Risikomanagement und Corporate Governance als systematische Einheit angesehen werden. Corporate Governance beschreibt das Rahmenwerk von Regeln und Richtlinien, die bei der Kontrolle und Führung eines Unternehmens eingehalten werden sollen. Das Risikomanagement stellt den strukturierten Prozess im Umgang mit Chancen und Risiken dar und die Compliance dient der effektiven Erfüllung des Rahmenwerks der Corporate Governance.[4]

Der Datenschutz kann als Bestandteil der betrieblichen Compliance somit als Teilbereich angesehen werden, der den gesetzlichen Bestimmungen entsprechen und darüber hinaus den selbstauferlegten Zielen und Vorgaben der Unternehmensleitung gerecht werden muss. Unternehmen müssen ein System implementieren, das bei jeglicher unternehmerischer Tätigkeit gegenüber den jeweiligen Stakeholdern den Datenschutzbestimmungen entspricht.

2.2 Der Datenschutz in der EU

2.2.1 Der Datenschutz als Grundrecht und die Datenschutzrichtlinie

Der Schutz personenbezogener Daten ist im EU-Recht als eigenständiges Grundrecht anerkannt und findet sich in Art 8 der EU-Grundrechtecharta. Dieser Artikel besagt:

- Jede Person hat das Recht auf Schutz der sie betreffenden persönlichen Daten.

[3] Vgl. Moosmayer, K.: Compliance – Praxisleitfaden für Unternehmen, 2. Auflage, München 2012, S. 1ff

[4] Vgl. Becker, W./Urlich, P., Corporate Governance und Controlling – Begriffe und Wechselwirkungen. In: Keuper, F./Neumann, F. (Hrsg.): Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien, 1. Auflage, Wiesbaden 2010, S. 7

- Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
- Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Die Besonderheit hinsichtlich der Behandlung des Schutzes personenbezogener Daten in der EU-Grundrechte-Charta kann darin gesehen werden, dass - im Gegensatz zu anderen internationalen Dokumenten im Bereich der Menschenrechte - der Datenschutz nicht nur als Erweiterung des Rechts auf Privatsphäre behandelt wird, sondern ein unabhängiges, eigenständiges Grundrecht darstellt. Die EU-Richtlinie 95/46/EG definiert personenbezogene Daten als alle Informationen über Personen, die direkt oder indirekt identifiziert werden können. Diese Richtlinie aus dem Jahre 1995 fungiert aktuell als wichtigstes Instrument der EU in Bezug auf den Schutz personenbezogener Daten und deren Verarbeitung. Diese „Datenschutzrichtlinie“ basiert auf den folgenden Grundprinzipien:

- Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen.
- Die Zwecke der Verarbeitung müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden.
- Die Verarbeitung hat den angestrebten Zwecken zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Außerdem müssen die Daten sachlich richtig sein und gegebenenfalls auf den neusten Stand gebracht werden.
- Personenbezogene Daten können nur dann rechtmäßig verarbeitet werden, wenn bestimmte, in der Richtlinie festgelegte Kriterien für die Verarbeitung erfüllt sind. Für die Überwachung der Einhaltung der Rechte ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen.
- Die Übermittlung der personenbezogenen Daten in Drittländer ist nur dann zulässig, wenn in diesen Ländern ein angemessenes Schutzniveau gewährleistet ist.
- Die EU und ihre Mitgliedstaaten müssen eine oder mehrere unabhängige Stellen vorsehen, die gewährleisten, dass die Vorschriften korrekt angewendet werden.

Die Datenschutzrichtlinie gilt nach Artikel 3 Abs 2 für die automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. In der Richtlinie 2002/58/EG wird die Datenschutzrichtlinie näher spezifiziert und um den Bereich der elektronischen Kommunikation ergänzt. Dadurch sollen die verschiedenen einzelstaatlichen Bestimmungen zum Schutz des Rechts auf Privatsphäre in Bezug auf personenbezogene Daten im Bereich der elektronischen Kommunikation harmonisiert werden. Diese Richtlinien sind an alle Mitgliedstaaten gerichtet und von diesen in nationales Recht umzusetzen.[5]

Da Richtlinien nur Zielvorgaben beinhalten und die praktische Umsetzung den Mitgliedstaaten überlassen bleibt, findet sich innerhalb der EU ein Flickwerk unterschiedlicher Regelungen. Dies betrifft etwa unterschiedliche Handhabungen bezüglich der Datenschutzbehörden, der Datenschutzbeauftragten oder von Sanktionen und führt dadurch zu inkongruenten Schutzniveaus in den verschiedenen Mitgliedstaaten.

2.2.2 Die Datenschutzbehörden

Art 28 Abs 1 S 1 der Datenschutzrichtlinie folgend, haben alle Mitgliedstaaten der EU eine einzelstaatliche Kontrollstelle benannt, um die Anwendung der datenschutzrechtlichen Bestimmungen im jeweiligen Hoheitsgebiet zu überwachen. Manche Mitgliedstaaten (z.B. Österreich) haben eine Datenschutzbehörde mit allgemeiner Zuständigkeit und weitere branchenspezifische Stellen installiert. Andere Staaten mit föderaler oder regionaler Organisation von Befugnissen (z.B. Deutschland) haben eine staatliche Kontrollstelle und mehrere regionale Kontrollstellen eingerichtet. In manchen Ländern (z.B. Finnland) wiederum kommt dem behördlichen Bürgerbeauftragten noch immer eine maßgebliche Bedeutung für den Schutz personenbezogener Daten zu. Bei diesen unterschiedlichen Implementierungen der Datenschutzbehörde ist darauf zu achten, dass diese ihre Aufgaben in völliger Unabhängigkeit wahrnehmen kann. In manchen Mitgliedstaaten (z.B. Deutschland) werden die Mitarbeiter der Datenschutzbehörden durch die

[5] Vgl. Agentur der Europäischen Union für Grundrechte, a.a.O., S. 14f

gesetzgebende Versammlung gewählt, während in anderen die Wahl in Form von Verfahren - die einen Konsens zwischen der Mehrheit und der Opposition fordern - stattfindet (z.B. Griechenland). Dadurch ist in den meisten Ländern ein gewisses Maß an Unabhängigkeit gewährleistet. Es gibt allerdings auch Ausnahmen in Ländern, die den Parlamentsparteien Ermessensentscheidungen bezüglich der Verteilung der Posten der Mitarbeiter der Datenschutzbehörden einräumen (z.B. Ungarn). Andere Länder wiederum haben die Kontrollstelle an das Justizministerium angegliedert (z.B. Dänemark), benennen diese direkt durch die Regierung (z.B. Irland) oder sehen ein kombiniertes Verfahren von Exekutive, Legislative und Judikative vor (z.B. Spanien). In all diesen Fällen ist jedoch zu beachten, dass die Regierung nicht die unmittelbare oder mittelbare Kontrolle über die Mehrzahl der berufenen Mitglieder innehaben darf. Die Mitgliedstaaten der EU waren außerdem dazu angehalten, diese Kontrollstellen mit den allgemeinen Befugnissen nach Art 28 der Datenschutzrichtlinie auszustatten. Dies sind unter anderem Beratungsbefugnisse, Untersuchungsbefugnisse und Befugnisse zur Befassung mit Eingaben. Diese Kontrollrechte wurden jedoch nicht in allen Staaten in gleicher Weise umgesetzt, daher verfügen die Datenschutzbehörden in einigen Ländern nur über begrenzte Instrumentarien zur Durchsetzung. Diese Problematik ist von den jeweiligen Ländern zu lösen. In einigen Ländern (z.B. Vereinigtes Königreich) wurde die präventive Rolle der Kontrollstellen betont, während in anderen Nationen (z.B. Lettland) das Hauptaugenmerk auf die nachträgliche Durchsetzungs- und Kontrollbefugnis bei Verstößen gelegt wurde. Einige Länder (z.B. Italien) fanden einen Mittelweg und setzten sowohl auf präventive Kontrolle als auch auf reaktive Zwangsgewalt durch Bestrafung. Dies ergibt für die nationalen Datenschutzbehörden unterschiedliche Handlungsspielräume bezüglich ihrer Überwachungs- und Durchsetzungsfunktionen, beispielsweise hinsichtlich ihrer Untersuchungsbefugnisse.[6]

[6] Vgl. Agentur der Europäischen Union für Grundrechte, a.a.O., S. 20ff,

Mitgliedstaat	Anforderung von Informationen und Unterlagen	Zugang zu Datenbanken und Archivierungssystemen	Durchsuchung von Räumlichkeiten und Beschlagnahme ohne richterliche Anordnung	Durchsuchung von Räumlichkeiten und Beschlagnahme mit richterlicher Anordnung	Durchführung von Audits
Belgien	●	●	●		●
Bulgarien	●	●	●		●
Dänemark	●	●	●		●
Deutschland	●	●	●	●*	●
Estland	●	●	●		●
Finnland	●	●	●		●
Frankreich	●	●		●	●
Griechenland	●	●	●		●
Irland	●	●	●		●
Italien	●	●	●**	●	●
Lettland	●	●	●		●
Litauen	●	●	●		●
Luxemburg	●	●	●		●
Malta	●	●		●	●
Niederlande	●	●	●		●
Österreich	●	●	●		●
Polen	●	●	●		●
Portugal	●	●	●		●
Rumänien	●	●			●
Schweden	●	●	●		●
Slowakei	●	●	●		●
Slowenien	●	●	●		●
Spanien	●	●	●		●
Tschechische Republik	●	●	●		●
Ungarn	●	●	●		●
Vereinigtes Königreich	●			●	●***
Zypern	●	●	●		●

Anmerkungen: *Diese Feststellung beschränkt sich auf den Bundesdatenschutzbeauftragten. Sie bezieht sich nicht auf die Datenschutzbeauftragten auf Länderebene und die für den privaten Bereich zuständigen Kontrollstellen.
**Normalerweise ist in Italien keine gerichtliche Anordnung erforderlich, wenn eine Durchsuchung in der Wohnung einer Person oder in einer anderen privaten Wohnstätte mit Zustimmung dieser Person durchgeführt wird. Ansonsten ist eine richterliche Genehmigung erforderlich.
***Die Datenschutzbehörde im Vereinigten Königreich kann Prüfungen nur auf Ersuchen des für die Verarbeitung Verantwortlichen durchführen; gegen den Willen eines für die Verarbeitung Verantwortlichen können keine Prüfungen vorgenommen werden. Die Befugnis kann somit nicht zur Kontrolle der Einhaltung der gesetzlichen Bestimmungen genutzt werden.

Abbildung 1: Untersuchungsbefugnisse[7]

2.2.3 Datenschutz-Registrierungen und interne Datenschutzbeauftragte

Der Begriff „Verarbeitung von personenbezogenen Daten“ nach Art 2 der Datenschutzrichtlinie definiert ein breites Spektrum von Sachverhalten. Dieses

[7] Agentur der Europäischen Union für Grundrechte, a.a.O., S. 23

umfasst u.a. das Erheben, Speichern, Aufbewahren, Anpassen, Abfragen, Weitergeben oder Vernichten von Daten. In den Art 5 – 8 der Datenschutzrichtlinie finden sich die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung von Daten und in den Art 18 – 20 die Bestimmungen über die Pflicht zur Meldung bei den Kontrollstellen und die Vorabkontrolle von Verarbeitungen. Die Bestimmungen wurden in den meisten Ländern zufriedenstellend in den nationalen Rechtsrahmen transferiert und dadurch eine wirksame Durchsetzung der Richtlinie gewährleistet. Es gibt jedoch auch negative Beispiele von EU-Ländern, deren nationale Regelungen der Datenschutzrichtlinie nicht gerecht werden. In manchen Ländern sehen sich die nationalen Datenschutzbehörden einem administrativen Aufwand gegenüber, welchen sie mit dem vorhandenen Personal nicht bewältigen können. Dadurch sind die Zielvorgaben der Datenschutzrichtlinie nicht flächendeckend in der gesamten EU gewährleistet, da in manchen Staaten die maßgeblichen Bestimmungen zwar umgesetzt wurden, die praktische Umsetzung jedoch mangelhaft ist. Defizite finden sich in einigen Ländern auch im Bereich der Registrierungspflicht, welche ein zentrales Element der Datenschutzrichtlinie darstellt und besonders in Bezug auf hochsensible Daten von besonderer Relevanz ist. Deutschland kann als positives Beispiel genannt werden, da die Datenschutzrichtlinie sowohl auf Bundes- als auch auf Landesebene wirksam umgesetzt wurde. Nichtöffentliche Stellen sind in der Bundesrepublik verpflichtet, automatisierte Datenverarbeitungen vorab der Kontrollstelle oder dem zuständigen Datenschutzbeauftragten zu melden. Die Registrierungspflicht entfällt, wenn der für die Verarbeitung Verantwortliche einen internen Datenschutzbeauftragten benannt hat. Zahlreiche Unternehmen kommen jedoch in der Praxis der Verpflichtung zur Einstellung eines internen Datenschutzbeauftragten nicht nach oder hindern diesen an einer effektiven Ausübung seines Aufgabenbereiches. In den meisten Ländern werden von den internen Datenschutzbeauftragten keine spezifischen Kenntnisse oder besondere Erfahrungen verlangt. Manche Länder sehen überhaupt keine Anforderungen für die Benennung von Datenschutzbeauftragten vor. In anderen Mitgliedstaaten (z.B. Deutschland) werden durch die gesetzliche Regelung ausdrückliche Bestimmungen zur Unabhängigkeit festgelegt und von den internen Datenschutzbeauftragten einschlägige Kenntnisse und Erfahrungen gefordert, diese allerdings auch nicht

weiter ausgeführt und näher definiert. Nur in Irland und Lettland muss ein interner Datenschutzbeauftragter konkret einen Hochschulabschluss in Rechtswissenschaften, Verwaltungswissenschaften oder Informationstechnologie vorweisen oder gleichwertig qualifiziert sein. Die Problematik der unterschiedlichen Qualifikation der Datenschutzbeauftragten in einzelnen Mitgliedstaaten ergibt sich dadurch, dass die EU für die Benennung in der Datenschutzrichtlinie keine verpflichtenden Standards vorgesehen hat.[8]

2.2.4 Sanktionen

Die Mitgliedstaaten wurden durch die Datenschutzrichtlinie verpflichtet Rechtsbehelfe und Sanktionen im nationalen Recht zu etablieren, welche die Einhaltung der Datenschutzbestimmungen gewährleisten. Da auch hier nur Zielvorgaben festgelegt wurden, die konkrete Anwendung jedoch den einzelnen Ländern überblieb, sind auch in diesem Bereich erhebliche Unterschiede in einzelstaatlichen Regelungen zu finden. Diese betreffen sowohl die Möglichkeit zur Rechtsdurchsetzung als auch die direkte Durchführung von Bestrafungen. Die Rechtsbehelfe teilen sich in administrative Rechtsbehelfe vor der Datenschutzbehörde, außerordentliche Rechtsbehelfe vor der Kontrollstelle und gerichtliche Rechtsbehelfe, die durch eine Klage vor ordentlichen Gerichten durchgesetzt werden. Letztere können von natürlichen Personen im Zusammenhang mit einem direkten Verstoß oder einer allgemeinen Beschwerde vor der Datenschutzbehörde erhoben werden. Faktisch besteht in mehreren Ländern die Möglichkeit zur Nutzung von Rechtsbehelfen, allerdings werden diese in der Praxis von Klägern kaum genutzt. Nur in wenigen Ländern (z.B. Italien) haben die betroffenen Personen die Möglichkeit, Rechtsstreitigkeiten entweder vor Gericht vorzutragen oder Beschwerden bei den Datenschutzbehörden einzureichen.

Nach Art 24 der Datenschutzrichtlinie sind die Mitgliedstaaten außerdem verpflichtet, Sanktionen für Verstöße zu setzen. Diese Bestimmungen divergieren durch den Einfluss der unterschiedlichen nationalen Straf- und Verwaltungsregelungen und tragen daher auch einen erheblichen Teil zum zersplitterten Bild des

[8] Vgl. Agentur der Europäischen Union für Grundrechte, a.a.O., S. 30ff

Datenschutzrechts in Europa bei. Dies wird durch die nachstehende Abbildung verdeutlicht, welche die unterschiedlichen Möglichkeiten zur Durchsetzung von Sanktionen in einzelnen Mitgliedstaaten aufzeigt.[9]

Mitgliedstaat	Von den Datenschutzbehörden verhängte Geldbußen	Von den Justizbehörden verhängte Geldstrafen	Von den Justizbehörden verhängte Freiheitsstrafen
Belgien		●	
Bulgarien	●		
Dänemark		●	●
Deutschland	●*	●	●
Estland	●	●	●
Finnland	●	●	●
Frankreich	●	●	●
Griechenland	●	●	●
Irland	●	●	
Italien	●	●	●
Lettland	●		
Litauen		●	
Luxemburg	●	●	
Malta	●	●	●
Niederlande	●	●	●
Österreich		●	●
Polen		●	●
Portugal	●		●
Rumänien	●	●	
Schweden		●	●
Slowakei	●	●	●
Slowenien	●	●	●
Spanien	●		
Tschechische Republik	●		
Ungarn		●	●
Vereinigtes Königreich		●	●
Zypern	●	●	

*Anmerkung: *Im Jahr 2008 wurden beispielsweise Bußgelder in Höhe von 1,4 Mio. EUR gegen das Handelsunternehmen LIDL verhängt und von diesem akzeptiert.*

Abbildung 2: Sanktionen[10]

[9] Vgl. Agentur der Europäischen Union für Grundrechte, a.a.O., S. 33ff

[10] Agentur der Europäischen Union für Grundrechte, a.a.O., S. 36

2.2.5 Die Datenschutzrichtlinie und ihre Folgen

Zusammenfassend betrachtet kann festgehalten werden, dass sich der Datenschutz EU-intern an im globalen Vergleich hohen Zielen ausrichtet. Durch die unterschiedliche Umsetzung - bedingt durch die unpräzisen Vorgaben zur Durchführung der Datenschutzrichtlinie - findet sich innerhalb der EU jedoch ein Fleckenteppich divergierender nationaler Bestimmungen und auseinanderklaffender Datenschutzniveaus. Dieser Umstand schwächt den europäischen Datenschutz als Ganzes, da durch Schwachstellen in einzelnen Mitgliedstaaten der gesamte EU-Raum gefährdet ist und sich daher die grundlegende Frage stellt, ob die Regelung des Datenschutzes innerhalb der EU in Form einer Richtlinie eine glückliche Entscheidung war. Da der Datenschutz als Grundrecht ein besonderes Schutzbedürfnis repräsentiert, scheint eine starke EU-weite Regelung wünschenswert und vor dem Hintergrund des freien EU-Binnenmarkts von bedeutender praktischer Relevanz zu sein. Durch die unterschiedliche Umsetzung der Datenschutzrichtlinie hat sich in Europa in den letzten zwei Jahrzehnten jedoch ein Datenschutz-Konstrukt gebildet, das jedenfalls eine Einzelfallbewertung in den jeweiligen Mitgliedstaaten erfordert und keine pauschale Betrachtung der EU als Gesamtgebilde ermöglicht.

2.3 Aktuelle Entwicklungen

2.3.1 Die EU-Datenschutz-Grundverordnung (EU-DS-GVO) als Instrument zur Vereinheitlichung

Die EU verhandelt seit 2012 eine Reform, die den Datenschutz in Europa den modernen Gegebenheiten anpassen soll und eine Vereinheitlichung der Datenschutzregelungen in Europa anstrebt.[11] Diese Reform findet sich aktuell im Entwurf-Stadium und die endgültige Form der Umsetzung kann noch nicht

[11] Vgl. Europäische Kommission, Pressemitteilung: Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, http://europa.eu/rapid/press-release_IP-12-46_de.htm?locale=en, abgefragt am 22.6.2015

vorausgesagt werden. Nichtsdestotrotz lassen sich die wichtigsten Ziele definieren und so besteht die Möglichkeit, die Folgen der EU-DS-GVO für Unternehmen zumindest abzuschätzen. Jedenfalls zu beachten ist, dass die EU-DS-GVO durch ihren Typus als Verordnung direkte Geltung in den Mitgliedstaaten entfalten wird und somit die unterschiedlichen nationalen Umsetzungen beseitigen und den Datenschutz in Europa auf ein gemeinsames, starkes Level heben soll. Die wichtigsten geplanten Änderungen sollen in der Folge überblicksweise dargestellt werden.

2.3.2 Verschärfte Sanktionen

Durch die EU-DS-GVO sollen die Strafen bei Zuwiderhandeln drastisch erhöht werden. So sah etwa schon der Vorschlag der Kommission eine Strafhöhe von bis zu einer Million Euro oder zwei Prozent des weltweiten Konzernumsatzes vor und das Parlament ging sogar von einer Strafhöhe von 100 Millionen Euro oder fünf Prozent des weltweiten Konzernumsatzes aus. In welchem Bereich sich der Strafrahmen genau ansiedeln wird, ist noch nicht festzumachen, allerdings können Unternehmen von einer drastischen Verstärkung der Sanktionen ausgehen. In diesem Zusammenhang sieht die EU-DS-GVO außerdem Maßnahmen vor, die Datenschutzverstößen vorbeugen. Diesbezüglich wird von Unternehmen die Einhaltung der Prinzipien „Privacy by Design“ und „Privacy by Default“ gefordert, welche ein Durchführen von Datenschutz-Folgeabschätzungen vor der Einführung datenverarbeitender Systeme und die Festlegung von Richtlinien für den Umgang mit Datenschutzverstößen bedeuten. Durch diese vorbeugenden Maßnahmen können im Falle eines Verstoßes die Geldbußen reduziert werden.[12]

2.3.3 Stärkung der Eigenverantwortlichkeit und der verpflichtende Datenschutzbeauftragte

Im Zuge der EU-DS-GVO soll außerdem die Eigenverantwortlichkeit der Unternehmen gestärkt werden, indem etwa Meldeverfahren auf spezifische

[12] Vgl. Knyrim, R./Trieb, G., Das künftige EU-Datenschutzrecht - Neue Anforderungen an die betriebliche Compliance. In: Burger-Scheidlin, M. et al. (Hrsg.): Compliance Praxis, Ausgabe 2, Wien 2014, S. 30

Anwendungsfälle reduziert werden. Dies stellt vor allem Unternehmen in verflochtenen und größeren Unternehmensgruppen vor die schwierige Aufgabe, sich mit den einzelnen Aspekten der unterschiedlichen Datenanwendungen auseinanderzusetzen, um Sanktionen zu vermeiden. Ein verpflichtender Datenschutzbeauftragter soll für Unternehmen vorgesehen werden, in denen Daten von zumindest 5000 Personen gespeichert sind. Der ursprüngliche Entwurf hatte vorgesehen, dass ein Datenschutzbeauftragter erst ab 250 Beschäftigten zwingend einzurichten ist, was in Österreich etwa nur 0,3 Prozent der Unternehmen betreffen würde.[13]

Die Erhöhung der Strafen in Kombination mit einem Anheben der Eigenverantwortlichkeit der Unternehmen scheint den Zweck zu verfolgen, Unternehmen indirekt zu datenschutzkonformen Verhalten zu zwingen und gleichzeitig administrative Schritte abzubauen. Dadurch wird den Unternehmen bei oberflächlicher Betrachtung mehr Handlungsspielraum gewährt, aber auf den zweiten Blick ein höheres Risiko auferlegt. Dieser Umstand könnte die Wichtigkeit der Position des Datenschutzbeauftragten stärken, daher kann die Frage nach der Regelung des verpflichtenden Datenschutzbeauftragten in der EU-DS-GVO als eine der zentralen Themen dieser geplanten Verordnung angesehen werden. Dabei scheint es fraglich, ob der Maßstab für die verpflichtende Einstellung eines solchen an der Anzahl der Beschäftigten ausgerichtet werden sollte, da auch Unternehmen mit wenigen Mitarbeitern aufgrund ihres Unternehmensinhalts große Datenmengen speichern können und wiederum größere Unternehmen anderer Branchen einen vergleichsweise geringen Datenumsatz aufweisen können. Die Lösung ist vermutlich ein Mittelweg, indem man zur Anzahl der Beschäftigten weitere Faktoren – wie die oben genannte Anzahl der betroffenen Personen – hinzuzieht und so einen realitätsnahen Maßstab schafft.

2.3.4 Datenschutzzertifizierung

Die Datenschutzverordnung sieht in den aktuellen Vorschlägen der Ratsarbeitsgruppen auch vielversprechende Lösungen zur Datenschutzzertifizierung

[13] Vgl. Knyrim, R./Trieb, a.a.O., S. 31

vor. Es soll unter anderem möglich werden, mit Vorlage eines anerkannten Zertifikats im Sinne von Art 39 des Entwurfs zur EU-DS-GVO zu belegen, dass die Vorgaben zum Datenschutz per Produktgestaltung und zum Datenschutz per Voreinstellung eingehalten wurden (Art 23 Abs 2a GVO-E). Außerdem soll durch Zertifikatsvorlage die Zuverlässigkeit der technisch-organisatorischen Vorkehrungen nachgewiesen werden können (Art 26 Abs 2aa GVO-E).[14]

2.3.5 Erweiterung des Geltungsbereichs der europäischen Datenschutzbestimmungen

Jegliche außerhalb der EU stattfindende Bearbeitung von personenbezogenen Daten, die EU-Bürger betreffen, soll künftig den EU-Vorschriften unterliegen.[15] Dadurch werden auch außereuropäische Unternehmen gezwungen, sich den europäischen Datenschutzstandards anzupassen, wenn sie auf dem EU-Markt aktiv sind. Diese Regelung kann somit als einschneidende Veränderung für große globale Unternehmen – wie etwa die US-amerikanischen Riesen Facebook, Google oder Apple – gesehen werden, da durch diese Regelung bisher bestehende Schlupflöcher - in Bezug auf die Sammlung von Daten europäischer Bürger - beseitigt werden sollen.

2.3.6 Das „Recht auf Vergessen-werden“

Durch das „Recht auf Vergessen-werden“ soll den EU-Bürgern ein größerer Handlungsspielraum hinsichtlich der Beherrschung der Datenschutzrisiken im Umgang mit Onlinediensten ermöglicht werden. Dadurch soll jeder EU-Bürger das Recht auf Löschung seiner Daten haben, wenn keine legitimen Gründe für deren Vorhaltung bestehen.[16]

---

[14] Vgl. Richter, F., Dialog: Datenschutz als Wettbewerbsvorteil . vielleicht klappt es doch… In: Berliner Datenschutzrunde: Initiative für einen modernen Datenschutz, https://www.berliner-datenschutzrunde.de/node/177, abgefragt am 28.6.2015

[15] Vgl. Europäische Kommission, Pressemitteilung: Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, http://europa.eu/rapid/press-release_IP-12-46_de.htm?locale=en, abgefragt am 22.6.2015

[16] Vgl. Europäische Kommission, a.a.O.

2.3.7 Das Recht auf Datenportabilität

Die Bürger sollen leichter auf ihre Daten zugreifen können und bei einem Wechsel zu anderen Anbietern die Möglichkeit haben, ebendiese Daten auf neue Anbieter zu übertragen. Durch diese Regelung wird der Wettbewerb unter den Anbietern solcher Dienste zunehmen.[17]

2.4 Der Datenschutz aus Unternehmenssicht

Der Datenschutz als Bestandteil betrieblicher Compliance stellt Unternehmen somit - sowohl vor als auch nach der geplanten EU-DS-GVO - vor komplexe Problemstellungen. Die Unternehmensleitung hat Sorge zu tragen, dass das CMS wirksam Datenschutzverstöße verhindert oder zumindest Vorfälle unverzüglich anzeigt, um Gegenmaßnahmen einleiten zu können und Schäden zu vermeiden. Das CMS muss bezüglich seiner Überwachungstätigkeit selbst den Datenschutzbestimmungen entsprechen und ein Gesamtbild der Unternehmung vermitteln, das den gesetzlichen und gesellschaftlichen Werten entspricht. Die Implementierung eines solchen CMS fordert von den Unternehmen einen hohen organisatorischen und finanziellen Aufwand. Durch die Datenschutzrichtlinie und deren unterschiedliche Umsetzung in einzelnen Mitgliedstaaten der EU verkompliziert sich die wirksame Umsetzung für Unternehmen mit transnationalem Charakter und stellt diese vor noch komplexere Aufgaben, da verschiedenartige nationale Regelungen zu beachten sind. Die Mitgliedstaaten der EU weisen untereinander erhebliche Unterschiede bezüglich des Datenschutzniveaus auf und eröffnen so auch außereuropäischen Unternehmen Möglichkeiten, sich nicht am europäischen Höchstniveau orientieren zu müssen. Dieses Ungleichgewicht soll durch die EU-DS-GVO beseitigt werden und dadurch der europäischen Datenschutz auf ein flächendeckend hohes Niveau angehoben werden, an das sich auch außereuropäische Unternehmen halten müssen. Die geplanten Änderungen stellen Unternehmen wiederum vor neue Herausforderungen und erhebliche Kosten für die Umsetzung. Höhere Bußgelder und strengere, flächendeckende Regelungen auf der

[17] Vgl. Europäische Kommission, a.a.O.

einen, ein beabsichtigtes Anheben der Eigenverantwortlichkeit von Unternehmen auf der anderen Seite. Die aktuellen Entwicklungen in Europa machen es für datenverarbeitende Unternehmen unumgänglich, sich mit dem Thema Datenschutz auseinanderzusetzen und sich den neuen Gegebenheiten anzupassen. Die Datenschutz-Compliance wird daher im Allgemeinen weiterhin beschwerliche Pflicht angesehen, die hohe Kosten und hohen organisatorischen Aufwand verursacht.

3 Der Datenschutz als Faktor der Wertschöpfung

3.1 Wertschöpfung

Das Wort „Wertschöpfung“ ist ein Begriff der Betriebswirtschaftslehre, der schon lange als Beurteilungsmaßstab für wirtschaftliches Handeln herangezogen wird. Wertschöpfung bedeutet grundsätzlich die Differenz zwischen den Bruttoerträgen und den Vorleistungen eines Unternehmens und misst somit die Eigenleistung der Betriebe und trägt dadurch - ergänzend zu den betrieblichen Erfolgsgrößen Umsatz und Gewinn - zur Analyse des betrieblichen Leistungsprozesses bei.[18]

„Die Wertschöpfungssrechnung kann aus der Brutto-Erfolgsrechnung entwickelt werden. Das vom Betrieb erzeugte Gütereinkommen ergibt sich aus den gesamten Erlösen (den nach außen abgegebenen Güterwerten), von denen die „Vorleistungskosten“ (die von außen hereingenommenen Güterwerte, d.h. Leistungen vorgelagerter Produktionsstufen) abgezogen werden. Das vom Betrieb erzeugte Gütereinkommen ist gleich dem vom Betrieb erzeugten Geldeinkommen, der Summe von Arbeitserträgen, Gemeinerträgen (Steuern und Abgaben) und Kapitalerträgen (Saldo).“[19]

Die Wertschöpfung umfasst somit nicht nur den Gewinn, der durch unternehmerisches Handeln entsteht, sondern bezieht jegliche Leistung des

[18] Vgl. Kroeber-Riel, W., Die betriebliche Wertschöpfung: Unter besonderer Berücksichtigung des Handels. In: Schnutenhaus, O. (Hrsg.): Vertriebswirtschaftliche Abhandlungen des Instituts für industrielle Verbrauchsforschung und Vertriebsmethoden an der Technischen Universität Berlin, Heft 6, Berlin 1963, S. 15f, S. 30

[19] Gabler Wirtschaftslexikon, Stichwort: Wertschöpfung. In: Springer Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Archiv/54898/wertschoepfung-v8.html, abgefragt am 25.6.2015

Unternehmens mit ein. Dies können Kosteneinsparungen durch effizientes unternehmerisches Handeln, Chancen durch Imageverbesserungen oder die Steigerung des Gewinns durch effektives Wahrnehmen von Marktpotentialen sein.

3.2 Schadensminimierung

Da der Datenschutz als Bestandteil betrieblicher Compliance im Allgemeinen negativ betrachtet wird, scheint ein möglicher Nutzen auf den ersten Blick vor allem in der Verhinderung von negativen Effekten zu liegen. Den Kosten für die Errichtung eines datenschutzkonformen CMS stehen Kosten für Bußgelder, Haftungsschäden und etwaigen Reputationsschäden gegenüber. Letztere können weit höher ausfallen als jene der Errichtung eines CMS und zwingen Unternehmen indirekt zu rechtskonformem Handeln.[20]

Der gesetzliche Rahmen kann somit als Untergrenze des Handlungsspielraums für Unternehmen bezüglich der Datenschutz-Compliance angesehen werden. Ein langfristiges Zuwiderhandeln wird sich kaum ein Unternehmen leisten können bzw. wollen, solange die Kosten für Bußgelder den Wert der gesetzeswidrig erlangten oder verarbeiteten Daten übersteigt. Die geplante erhebliche Anhebung der Strafsanktionen macht es für Unternehmen unumgänglich, sich mit möglichen Datenschutzverstößen auseinanderzusetzen und diesen im CMS verstärkt Beachtung zu schenken. Durch die geplante Vereinheitlichung werden erhebliche Umstellungen vor allem in denjenigen Ländern zu bewältigen sein, die bisher schwach sanktioniert haben und in denen sich die Unternehmen auf ein niedriges Schutzniveau eingestellt haben.

[20] Vgl. Muth, T., Erfolgsfaktor Compliance-Kultur. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 213f

3.3 Wertschöpfung durch Kosteneffizienz

3.3.1 Das Prinzip der Datensparsamkeit

Der Datenschutz wird allgemein als Einschränkung effektiver Nutzung von Whistleblowing-Systemen gesehen. Dabei kann es um die Nutzung personenbezogener Daten von Hinweisgebern, anderer Betroffener und Dritter gehen, die unter den rechtlich vorgegebenen Einschränkungen gesammelt werden. Als Grundsätze zur Erstellung eines solchen Systems nennt *Rohde-Liebenau*[21] die Prinzipien der Datensparsamkeit, der Verhältnismäßigkeit und der Transparenz. Die Datensammlung soll dabei minimiert werden und in solch einem Umfang stattfinden, dass nur betrieblich relevante Informationen gesammelt werden und personenbezogene Daten nur miteinbezogen werden, wenn dies zum Verständnis anderer Informationen vonnöten ist. Zusätzlich wird durch Transparenz bezüglich der eingesetzten Mittel Vertrauen in das System geschaffen und dadurch der Unsicherheit hinsichtlich der Folgen eines im Raum stehenden Tabubruchs entgegengearbeitet. Nach *Rohde-Liebenau*[22] werden die Prinzipien des Datenschutzes im Hinblick auf die Errichtung eines Whistleblowing-Systems somit nicht als hemmend, sondern sogar als fördernd angesehen.

Die Datensparsamkeit wird also in diesem Fall als effektivitätssteigerndes Prinzip angesehen, welches sich in einer Minimierung der Datensammlung widerspiegelt, dessen Untergrenze die betriebliche Relevanz darstellt. Diese Betrachtung kann auch auf andere Bereiche der Datensammlung übertragen und ihrem Zwecke nach weitergedacht werden. Auf der einen Seite stehen persönliche Interessen auf den Schutz personenbezogener Daten, auf der anderen Seite stehen die Interessen des Betriebes, relevante Informationen einzuholen. Der Fokus muss dabei auf das Stichwort „Relevanz“ gelegt werden. Unternehmen haben wohl kein Interesse daran

---

[21] Vgl. Rohde-Liebenau, B., Compliance² – einfache Antworten auf neue Anforderungen. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 47ff

[22] Vgl. Rohde-Liebenau, B., Compliance² – einfache Antworten auf neue Anforderungen. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 47ff

Informationen zu sammeln, die außerhalb ihres Interessenbereiches liegen, da dies einen unnötigen Aufwand darstellt, der dem Prinzip der Effektivität entgegensteht. Durch die Sammlung irrelevanter Massen von Daten ergeben sich für Unternehmen unnötige Kosten, denen keine wirtschaftliche Begründetheit gegenübersteht. Persönliche und betriebliche Interessen müssen nicht zwangsweise divergieren, sondern können sich an ähnlichen Prinzipien ausrichten. Das Prinzip der Datensparsamkeit kann somit sowohl im Einklang mit persönlichen als auch betrieblichen Interessen sein und kann bei effektiver Anwendung zu Kosteneinsparungen führen. Dementgegen stehen jedoch die Entwicklungen in Form der EU-DS-GVO, welche Einschränkungen des Prinzips der Datensparsamkeit zugunsten von Betrieben vorsehen und den persönlichen Interessen weniger Beachtung beimessen. [23] Dies lässt vermuten, dass das Prinzip der Datensparsamkeit weiterhin als Einschränkung der Handlungsfähigkeit von Unternehmen angesehen wird. Nichtsdestotrotz scheint das Argument einer effektiven Kostenersparnis auf Basis des Prinzips der Datensparsamkeit fundiert und begründet zu sein.

3.3.2 Vereinheitlichung des europäischen Datenschutzes als Chance für transnational tätige Unternehmen

Die Gestaltung einer Datenschutz-Compliance gestaltet sich nach *Schließmann*[24] besonders schwierig, wenn Unternehmen sich auf internationalen Terrain bewegen und sich einer Vielzahl von sich unterscheidenden nationalen Gesetzen und Regelungen gegenübersehen. Dies stellt transnational tätige Unternehmen vor große Herausforderungen hinsichtlich der Implementierung eines unternehmensweit wirksamen CMS, das sowohl den Anforderungen in einzelnen Nationen als auch der gesamtunternehmerischen Zielsetzung gerecht werden muss. Dabei sollen sowohl

[23] Vgl. Dietrich, S., Blog: EU-Datenschutzgrundverordnung – Prinzip der Datensparsamkeit wird aufgeweicht. In: Security & Recht, https://blog.app-arena.com/2015/06/eu-datenschutzgrundverordnung-prinzip-der-datensparsamkeit-wird-aufgeweicht/, abgefragt am 22.6.2015

[24] Vgl. Schließmann, C., Compliance im Kontext internationaler Strukturen, Geschäftsmodelle und Wertschöpfungsprozesse. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 142

die Mitarbeiter als auch internationale Geschäftspartner und Stakeholder an verpflichtende Verhaltensrichtlinien gebunden sein, um so einen transnationalen Kontext zu gewährleisten und nationenspezifisch einen risikominierenden Handlungsrahmen setzen zu können.

Die Problematik ergibt sich für transnational tätige Unternehmen demnach durch die Zersplitterung der rechtlichen Bestimmungen und die kulturellen Unterschiede einzelner Länder. Innerhalb der EU ist der Datenschutz an gewisse Mindeststandards gekoppelt und genießt daher einen im internationalen Vergleich hohen Stellenwert. Allerdings findet sich innereuropäisch eine zersplitterte Rechtslage, die es erforderlich macht, die Gesetzeslage jedes betroffenen Mitgliedstaates einzeln zu beurteilen und zu analysieren. Dies bedeutet für europäische Unternehmen hohe Anforderungen bei der Implementierung eines CMS und durch die unterschiedlichen Umsetzungen der Datenschutzbestimmungen innerhalb der EU einen zusätzlichen Aufwand für Unternehmen, die über nationale Grenzen hinweg agieren.

Durch die Vereinheitlichung des Datenschutzes innerhalb der EU sollten sich für transnational tätige Unternehmen signifikante Einsparungspotenziale bei der Gestaltung eines flächendeckenden CMS ergeben, da auf eine einheitliche Linie gesetzt werden kann. Diese Einsparungspotenziale müssen jedoch vor dem Hintergrund der Gesamtkosten für die Umsetzung der geplanten Regelungen der EU-DS-GVO kritisch betrachtet werden. Diesbezüglich können sich erhebliche Unterschiede zwischen Unternehmen verschiedener Größe ergeben, daher ist eine Bewertung grundsätzlich einzelfallbezogen vorzunehmen. In einer isolierten Betrachtungsweise scheint die Möglichkeit zur Einsparung für transnational tätige Unternehmen bei der Durchführung eines staatenübergreifenden CMS durch die Einsetzung der EU-Datenschutz-Grundverordnung generell plausibel.

3.4 Wertschöpfung durch Realisieren von Wettbewerbsvorteilen

3.4.1 Chancen durch ein wirksames CMS

Schlüssig scheint die Annahme, dass sich durch ein wirksames und datenschutzkonformes CMS die Realisierbarkeit von wirtschaftlichen Chancen erhöht. Zwar stellt sich die Problematik der Messbarkeit des direkten Zusammenhangs zwischen einem wirksamen CMS und Aktienkursen, jedoch scheint eine höhere Vertrauenswürdigkeit durch nachgewiesene Effekte bei ähnlich gelagerten Normen und Standards gegeben zu sein. Dies wären etwa Gütesiegel aus dem Umwelt- oder Fairtrade-Bereich, welche die Vermutung ähnlich positiver Auswirkungen durch ein wirksames CMS nahelegen. Diese positive Stellung gegenüber Konkurrenzunternehmen kann zu einer Bevorzugung in Fragen der Vergabe von Aufträgen durch Unternehmer und Investoren führen und dadurch die Wertschöpfung im Unternehmen steigern. Zu beachten ist allerdings, dass dieser Effekt nachlässt, sobald ein derartiges Handeln zum allgemeinen Standard wird und sich dadurch die positiven Effekte auflösen.[25]

Die Problematik der Messbarkeit macht es für Unternehmen somit schwierig, Chancen und Risiken von datenschutzbezogenem Handeln zu quantifizieren und gegeneinander abzuwägen. Können Bußgelder und Strafen noch leicht prognostiziert und abgeschätzt werden, sind ideelle Aspekte - welche zu Chancen führen können - schwer einzuschätzen und stützen sich selten auf rational bewertbare Daten. Die Übertragung der Annahme von oben angeführten wünschenswerten Effekten von ähnlich gelagerten Studien auf datenschutzkonformes Handeln scheint jedoch zielführend zu sein. Gerade wenn ein Unternehmen sich im Bereich anderer Faktoren mit Konkurrenzunternehmen im Gleichschritt befindet, können kleine Faktoren große Auswirkungen haben. Dies scheint den Mehraufwand für eine

[25] Vgl. Muth, T., Erfolgsfaktor Compliance-Kultur. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 214f

positive Außendarstellung durch ein funktionierendes CMS zu rechtfertigen, speziell vor dem Hintergrund, dass man ohnehin an Kosten gebunden ist, die sich durch die rechtlichen Verpflichtungen ergeben. Dem steht wohl auch das Abflachen der Effekte bei angepassten Handlungsweisen von Konkurrenten nicht entgegen, da die Zeitspanne des Wettbewerbsvorteils genutzt wird und man sich im Zeitpunkt der Standardisierung zumindest nicht der Gefahr einer negativen Außendarstellung gegenübersieht. Diesbezüglich sind natürlich auch die rechtlichen Entwicklungen zu beachten, da ein Früherkennen von späteren Zwangsregulierungen zu kurzfristigen Wettbewerbsvorteilen führen kann, ohne dass es sich langfristig gesehen auf die Kosten niederschlägt. Wenn ein Unternehmen im Frühstadium rechtliche Tendenzen erkennt, die Anpassungen im Bereich der Compliance erforderlich machen, kann es durch sofortiges Handeln kurzfristige Chancen durch die positive Außendarstellung nutzen und die Änderungen durch Kosten decken, die zum späteren Zeitpunkt ohnehin fällig gewesen wären. Ein zukunftsorientiertes Handeln kann somit langfristig Kosten minimieren und gleichzeitig Chancen kreieren, was sich im Bereich der Wertschöpfung niederschlagen kann.

3.4.2 Wettbewerbsvorteile gegenüber den USA durch das zunehmende Bewusstsein um den Wert von Daten

Die datenschutzrechtlichen Regelungen Europas unterscheiden sich immens von jenen der USA. In Europa hat der Schutz von Daten eine lange Tradition, was sich in einer Vielzahl von Gesetzen und übergreifenden Regelungen niederschlägt. Besonders in Deutschland oder Österreich sieht das System der Datensparsamkeit und Datenvermeidung ein enges Korsett an Regeln für das Verwenden von Daten vor. Bedingt durch kulturelle Unterschiede werden eben diese - vergleichsweise strengen - Regelungen vom Blickwinkel eines US-Amerikaners aus als bevormundend und einschränkend angesehen. Diese gelebte Kultur schlägt sich auch im US-amerikanischen Datenschutz nieder, welcher sich bei Weitem nicht auf europäischen Niveau befindet. Die Auseinandersetzung mit Datenschutz - in Europa historisch gewachsen und auf eine lange Tradition zurückblickend - ist auch in den USA spätestens seit den Snowden-Enthüllungen ein Thema, das sich zunehmend im Bewusstsein der US-Bürger festsetzt. Nichtsdestotrotz sind die Restriktionen für US-

amerikanische Firmen aktuell gering und durch die große Anzahl von Online-Applikationen auch für Europäer von enormer Relevanz. Durch die laschen Regelungen und den Zugriff auf europäische Bürge durch Online-Aktivitäten ergeben sich für die USA auf den ersten Blick enorme Wettbewerbsvorteile.[26] Dies scheint bei oberflächlicher Betrachtung begründet zu sein, da europäische Unternehmen durch die hiesigen Restriktionen Einschränkungen in Bezug auf personenbezogene Daten und deren Verwendung in Kauf nehmen müssen, die sie im Wettkampf mit US-Unternehmen kaum kompensieren können. Bei genauerer Betrachtung erweisen sich diese vermeintlichen Vorteile vor dem Hintergrund gesellschaftlicher und kultureller Entwicklungen jedoch als trügerisch.

Das US-amerikanische Softwarehaus *Symantec*[27] hat eine Studie über den Umgang mit Daten in Europa und das europäische Bewusstsein im Hinblick auf die Datenverwendung und deren wirtschaftlichen Wert durchgeführt. Diese Studie zeigt das Gefahrenpotenzial auf, welches für US-amerikanische Unternehmen im Bereich des Datenschutzes besteht und weist u.a. die geplante EU-DS-GVO als kritischen Wendepunkt für Unternehmen aus. Käufer werden - dieser Studie zufolge - in der Zukunft zu jenen Anbietern und Unternehmen wechseln, bei denen sie ihre persönlichen Daten bestmöglich geschützt sehen. Dies wird durch ein wachsendes Bewusstsein der Käufer über den wirtschaftlichen Wert ihrer Daten bestärkt und führt für die Unternehmen zur Notwendigkeit der Schaffung einer fundierten Vertrauensbasis.

Nimmt man diese Studie als repräsentatives Beispiel, ist den US-amerikanischen Firmen die Problematik eines sich wandelnden Umgangs mit personenbezogenen Daten durchaus bewusst. Verbraucher setzen sich mehr und mehr kritisch mit dem Thema Datenschutz auseinander und hinterfragen die Verwendung ihrer persönlichen Daten sowie deren wirtschaftlichen Wert. Es ist spürbar, dass Unternehmen wie Facebook und deren Umgang mit personenbezogenen Daten

[26] Vgl. Ufer, F., Blog: Big Data: Ist Deutschland international wettbewerbsfähig? In: Big Data Blog 2015, https://bigdatablog.de/2015/02/19/big-data-ist-deutschland-international-wettbewerbsfaehig/, abgefragt am 20.6.2015

[27] Vgl. Symantec, State of Privacy Report 2015, http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf, abgefragt am 20.6.2015

zunehmend kritisch betrachtet werden. Durch das steigende Bewusstsein über den Wert von Daten ist es für Unternehmen in Zukunft - noch mehr als heute - von entscheidender Bedeutung, sich mit dem Thema Datenschutz-Compliance vor dem Hintergrund gesellschaftlichen Wandels auseinanderzusetzen, um sich im Wettbewerb mit anderen Unternehmen nicht in einer kritische Position wiederzufinden. Auf eben solch einen Wandel scheint ein Großteil der europäischen Firmen weitaus besser vorbereitet zu sein, da das Niveau des Datenschutzes in weiten Teilen Europas ein signifikant höheres ist und die vorhandene Infrastruktur im Bereich der Datenschutz-Compliance somit einen wertvollen Asset darstellen kann. Ein steigendes Bewusstsein der Verbraucher über den Wert von Daten kann somit zu Wettbewerbsvorteilen für europäische Unternehmen im Konkurrenzkampf mit den USA – oder allgemein Ländern mit geringen Datenschutzstandard - führen.

3.4.3 Erzielen höherer Preise durch höheren Standard

Allgemein betrachtet kann also ein gesellschaftlicher Wandel in Bezug auf den Umgang mit Daten aus unternehmerischer Sicht zu Chancen führen. Dies betrifft nicht nur die Möglichkeit Präferenzen von Kunden bezüglich der Wahl eines Unternehmens zu ändern, sondern zusätzlich die Chance einen höheren Marktpreis für Produkte oder Dienstleistungen zu erzielen, die einen höheren Datenschutzstandard bieten. Diesbezüglich ist darauf zu achten ob ein Markt vorliegt, der ein unternehmerisches Handeln mit dieser Intention rechtfertigt. Dieser Umstand liegt im Speziellen dann vor, wenn Kunden bereit sind, einen höheren Preis für einen höheren Standard zu zahlen und die Konkurrenz in diesem Segment überschaubar ist. Ob eine Unternehmenspositionierung im Bereich des Datenschutzes im „Premiumsegment“ dauerhaft möglich ist, hängt vom Handeln der Konkurrenzunternehmen ab. Dabei scheint es fragwürdig, ob sich Unternehmen langfristig im „Billigsegment“ positionieren und geringen Datenschutz für kleineren Preis anbieten würden, da bei einem heiklen Thema wie dem Datenschutz solch eine Marktstrategie äußerst riskant zu sein scheint. Wahrscheinlicher ist es, dass sich die Datenschutzregelungen schrittweise angleichen und sich höhere Preise nur kurz- bis mittelfristig erzielen lassen.

3.4.4 Datenschutz als Marketinginstrument

Durch die oben genannten Umstände wird die zunehmende Möglichkeit deutlich, den Datenschutz als Marketinginstrument nutzen zu können. Unternehmen setzen innerhalb ihrer Marketing-Konzepte mehr und mehr darauf zu betonen, dass ihnen der Schutz der Kundendaten ein besonderes Anliegen ist. Dieser Trend ist in den verschiedensten Branchen vorzufinden und offenbart, dass Datenschutz mittlerweile von vielen Unternehmen als Chance gesehen wird, sich von der Konkurrenz abzuheben. Diese Tendenz findet sich nicht nur in Europa, sondern auch bei US-amerikanischen Big Playern wie Apple, das etwa Google kritisierte, zu viele Daten über Nutzer zu sammeln und ankündigte verstärkt Nutzerdaten lokal auf den Endgeräten statt zentral auf eigenen Servern zu speichern. Wenn sich ein Wettbewerb entwickelt, bei dem sich Unternehmen beim Datenschutz zu überbieten suchen, kann dies nur begrüßt werden. Derartige Marktmechanismen sind vor allem in den USA deutlich wirksamer als politische Forderungen oder nicht wirksam durchgesetzte Gesetze.[28]

Die Entwicklungen durch die EU-DS-GVO im Bereich der Datenschutzzertifizierung zeigen ebenfalls, dass dieser Thematik zunehmend Beachtung geschenkt wird. Datenschutzgütesiegel können als Marketing-Instrument verwendet werden, um sich von der Konkurrenz abzugrenzen bis dieser Effekt durch das Angleichen des Niveaus innerhalb der Konkurrenzsituation stagniert. Aus Kundensicht bietet sich die interessante Möglichkeit, ein höheres Datenschutzniveau durch indirektes Fördern des Wettbewerbs zu erreichen. Wenn ein ausreichendes Maß an Kundendruck bezüglich eines höheren Schutzniveaus vorhanden ist und sich einzelne Unternehmen von der Konkurrenz abzuheben suchen, können sich Marktmechanismen in Gang setzen, die den Schutz personenbezogener Daten auf eine höhere Ebene heben, ohne dass dazu gesetzliche Regulierungen notwendig sind. Dies könnte zu einer für den Kunden wünschenswerten Situation führen, in der sich das Datenschutzniveau allgemein weit über den gesetzlichen

[28] Vgl. Richter, F., Dialog: Datenschutz als Wettbewerbsvorteil . vielleicht klappt es doch… In: Berliner Datenschutzrunde: Initiative für einen modernen Datenschutz, https://www.berliner-datenschutzrunde.de/node/177, abgefragt am 28.6.2015

Mindestbestimmungen bewegt. Für Unternehmen bedeutet dies freilich sich ständig weiterzuentwickeln und die Standards an die aktuellen Gegebenheiten anzupassen.

3.4.5 Wettbewerbsvorteil für Europa durch die EU-Datenschutz-Grundverordnung

Die Wettbewerbsvorteile können nicht nur vor dem Hintergrund gesellschaftlichen Wandels betrachtet werden, sondern auch im Hinblick auf die Änderung des gesetzlichen Rahmens in Europa durch die EU-DS-GVO. Die geplanten Maßnahmen der Verordnung betreffen nicht nur europäische Unternehmen, sondern schließen ebenso US-Unternehmen ein, die Daten von europäischen Bürgern verwenden.[29] Bisher nutzten bekannter Weise viele US-Unternehmen wie Facebook die für europäische Verhältnisse schwachen Restriktionen in Irland, um dort ihre Töchter anzusiedeln und über das Safe-Harbour-Abkommen zwischen den USA und der EU massenweise Daten von EU-Bürgern zu sammeln. Durch eine Vereinheitlichung der europäischen Datenschutzbestimmungen werden auch US-Unternehmen gezwungen sich anzupassen, da das Marktortprinzip – ungeachtet des Unternehmensstandorts -alle Firmen miteinbezieht, die sich an den europäischen Markt richten. Unternehmen, die sich bereits einer fundierten Basis im Bereich der Datenschutz-Compliance bedienen können, haben dadurch einen augenscheinlichen Wettbewerbsvorteil gegenüber jenen, die sich bisher kaum mit Datenschutz auseinandersetzen mussten. Dies kann zum einen kurz- bis mittelfristige Vorteile im innereuropäischen Wettbewerb bringen, da auch hier das Niveau auf dem sich der Datenschutz bewegt durch die aktuell noch zersplitterte Rechtslage auseinandertriftet. Dadurch haben jene Länder einen Aufholbedarf, in denen bisher schwache Datenschutzstandards gegolten haben und Nationen mit traditionell hohen Anforderungen an den Datenschutz einen augenscheinlichen Wettbewerbsvorteil. Auf interkontinentaler Ebene kann die EU-DS-GVO als Chance für viele europäische Unternehmen gesehen werden, den Vorsprung durch die bereits vorhandene Infrastruktur gegenüber den USA zu nutzen.

---

[29] Vgl. von Lieven, S., Kommentar: EU-Datenschutz-Grundverordnung – Chance oder Risiko? In: Artegic Blog, https://www.artegic.de/eCRM/artegic-ECRM-DE/Aktuelles_Kommentar:.EU-Datenschutz-Grundverordnung...Chance.oder.Risiko._0cq-5gr.html, abgefragt am 20.6.2015

3.5 Erforderliche Rahmenbedingungen für die Wertschöpfung durch Datenschutz

3.5.1 Relevante Faktoren

Die bisherigen Erkenntnisse zeigen, dass es durchaus Anhaltspunkte gibt, die den Datenschutz als wertschöpfenden Faktor ausweisen. Dazu müssen jedoch gewisse Rahmenbedingungen gegeben sein, die Möglichkeiten zur Realisierung von Chancen bieten, die über ein rein kosteneffizientes Umsetzen der Datenschutzbestimmungen hinausgehen. Unternehmen sind daher gefordert, diese Chancen und das Vorliegen der erforderlichen Rahmenbedingungen zu erkennen und in ihrer strategischen Unternehmensausrichtung umzusetzen. Zu diesem Zweck müssen die entscheidenden Faktoren analysiert werden, um so ein Gesamtbild über die Situation zu erhalten. In der Folge wird versucht, dies durch ein schematisches Modell darzustellen, das die Analyseschritte für Unternehmen in eine logische Ordnung bringen soll. Dabei scheint eine Einteilung in folgende vier Bereiche sinnvoll:

- Analyse der gesetzlichen Rahmenbedingungen
- Analyse des eigenen Unternehmens
- Analyse der Kundensituation
- Analyse der Konkurrenzsituation

Diese vier Teilbereiche sollen in dieser Reihenfolge betrachtet werden und eine weitergehende Analyse der nachstehenden Bereiche nur erfolgen, wenn dies durch die Ergebnisse der vorangegangenen Betrachtung begründet erscheint.

3.5.2 Analyse der gesetzlichen Rahmenbedingungen

Der gesetzliche Rahmen stellt die Untergrenze für den Umgang mit dem Datenschutz dar. Unterschreitungen werden sanktioniert und sind daher auch wirtschaftlich nicht wünschenswert, da die Vorteile aus einer Zuwiderhandlung im Normalfall die Zahlung der äquivalenten Bußgelder nicht rechtfertigen. Durch die Entwicklungen in Form der EU-DS-GVO werden diese Maßnahmen voraussichtlich zusätzlich verschärft und dadurch der gesetzliche Rahmen als Mindestanforderung

an den Datenschutz gefestigt. Unternehmen stehen vor der komplexen Aufgabe, alle relevanten gesetzlichen Datenschutzbestimmungen ins jeweilige CMS einfließen zu lassen, um so Sanktionen zu vermeiden. Die gesetzlichen Bestimmungen unterliegen häufig auftretenden Wandel und das Erkennen von Trends, die ein Anpassen der Datenschutzregelung im Unternehmen erfordern, kann von entscheidender Bedeutung für den Unternehmenserfolg sein. Auf die Möglichkeit der Beeinflussung von Gesetzen durch Lobbying wird hier nicht näher eingegangen, da sich die analytische Betrachtung hier nur auf einzelnen Unternehmen im Konkurrenzkampf bezieht. Der gesetzliche Rahmen kann somit als vorgegebene - aber im Wandel der Zeit variierende - Konstante angesehen werden, die von Unternehmen nicht direkt beeinflusst werden kann und die Untergrenze für das unternehmerische Handeln in Bezug auf den Datenschutz darstellt.

3.5.3 Analyse des eigenen Unternehmens

Der Datenschutz spielt nicht in jedem Unternehmen eine Rolle, die über die Einhaltung der gesetzlichen Bestimmungen hinaus geht und einen Einfluss auf die Wertschöpfung haben kann. Relevant ist die genauere Behandlung des Datenschutzes nur für Unternehmen, die große Datenmengen verarbeiten und bei denen daher das Kundenvertrauen eine entscheidende Rolle im Wertschöpfungsprozess einnimmt. Die Unternehmensleitung muss sich daher die Frage stellen, ob der Umgang mit dem Datenschutz - sowohl im positiven als auch im negativen Sinn - Auswirkungen auf den Unternehmenserfolg haben kann. Dies kann im Zweifel bei jedem Unternehmen angenommen werden, das große Datenmengen verarbeitet und bei dem dieser Umstand den Kunden auch bewusst ist. Liegen diese Gegebenheiten nicht vor, ist eine weitere Analyse hinsichtlich einer möglichen Wertschöpfung durch den Datenschutz unnötig, da dieser in solch einem Fall keinen relevanten Faktor in der Wertschöpfungskette darstellt. Liegen jedoch begründete Anhaltspunkte für einen direkten Zusammenhang vor, ist eine weitere Analyse zielführend.

3.5.4 Analyse der Kundensituation

Nachdem die gesetzlichen Mindestanforderungen abgesteckt wurden und die Relevanz der Datenschutzregelung für die Wertschöpfung festgestellt wurde, sind die Erwartungen und Präferenzen auf Kundenebene zu analysieren. Liegt die Erwartung der Kunden in Bezug auf den Schutz ihrer persönlichen Daten über dem gesetzlichen Rahmen, ergibt sich für Unternehmen ein Handlungsspielraum, der zu wirtschaftlichen Chancen führen kann. Liegen die Kundenerwartungen jedoch unter den gesetzlichen Bestimmungen, kann der Datenschutz tatsächlich als reine Einschränkung des unternehmerischen Handelns angesehen werden, da die Einhaltung der Datenschutzbestimmungen in diesem Fall - zumindest wirtschaftlich - nicht gerechtfertigt ist. In der Praxis werden sich jedoch Kundenpräferenzen finden, die über dem gesetzlichen Datenschutzniveau liegen und so eine Anhebung der unternehmensinternen Datenschutzregelungen rechtfertigen. Unternehmen sind daher insbesondere gefordert, tiefgreifende gesellschaftliche Veränderungen im Umgang mit persönlichen Daten und deren Schutz frühzeitig zu erkennen, um mögliche Wertschöpfungspotentiale nutzen zu können. Wertschöpfungspotentiale sind also dann gegeben, wenn Kundenpräferenzen vorhanden sind, die über den gesetzlichen Mindestanforderungen liegen und für das betrachtete Unternehmen aufgrund seines Unternehmensinhalts von wirtschaftlicher Relevanz sind.

3.5.5 Analyse der Konkurrenzsituation

Liegen die wirtschaftlichen Gründe vor, sich hinsichtlich des Datenschutzes über dem gesetzlichen Regelungsrahmen zu bewegen, ist zudem die Konkurrenzsituation in die Analyse miteinzubeziehen. Bewegt sich die Konkurrenz im Bereich des Datenschutzes unter den Kundenerwartungen besteht die Möglichkeit, durch Anheben des Datenschutzniveaus im eigenen Unternehmen - kombiniert mit geschickten Marketing – einen USP zu generieren. In diesem Fall liegen klare Wertschöpfungspotentiale vor, aber auch in anderen Konstellationen ist die Konkurrenzsituation zu beachten. Liegt man mit den Datenschutzbestimmungen im eigenen Unternehmen sowohl unter den Kundenerwartungen als auch dem Niveau der Konkurrenzunternehmen, ist Handlungsbedarf gegeben, um nicht langfristig Kunden zu verlieren. Die Konkurrenzsituation ist somit jedenfalls zu beachten, sei es

um auf einen möglichen Rückstand reagieren zu können oder aber um Wertschöpfungspotentiale wahrnehmen zu können.

3.5.6 Zusammenfassende Betrachtung

Dieser Versuch eines Modells stellt freilich nur eine grobstrukturelle Betrachtung der Zusammenhänge dar und soll veranschaulichen unter welchen Bedingungen Wertschöpfungspotentiale durch den Datenschutz vorliegen können. Zusammenfassend betrachtet müssen Unternehmen in einem ersten Schritt eine Einschätzung vornehmen, welche die Wichtigkeit des Datenschutzes und dessen Einfluss auf die wirtschaftliche Beziehung zum Kunden definiert, um so festzustellen, ob ein Handeln über dem gesetzlichen Rahmen wirtschaftlich gerechtfertigt ist. Liegen diese Voraussetzungen vor, muss die Kunden- und die Konkurrenzsituation analysiert werden und daraus eine Entscheidung für das unternehmerische Handeln abgeleitet werden. Wertschöpfungspotentiale liegen im Speziellen dann vor, wenn die Kundenerwartungen an den Datenschutz über den gesetzlichen Mindestanforderungen und den Regelungen der Konkurrenzunternehmen liegen.

4 Fazit

Der europäische Datenschutz als Bestandteil betrieblicher Compliance stellt Unternehmen vor komplexe Herausforderungen und fordert einen hohen organisatorischen und finanziellen Aufwand. Dieser Umstand wird auch nach Durchführung der Datenschutzgrundverordnung bestehen bleiben. Allerdings sollten sich durch die geplanten Änderungen der EU-DS-GVO zahlreiche Erleichterungen für Unternehmen ergeben, da administrativer Aufwand abgebaut werden soll und durch die Vereinheitlichung der Bestimmungen ein einfacheres Umsetzen der Datenschutzbestimmungen im internationalen Raum ermöglicht werden soll. Bei der Betrachtung der Vorteile für Unternehmen ist aber jedenfalls eine Einzelfallbewertung vorzunehmen. Die allgemeine Anhebung und Vereinheitlichung des Datenschutzes wird vor allem jene Unternehmen vor Probleme und hohen Aufwand stellen, die sich bisher schwachen Datenschutzbestimmungen gegenübersahen und die Datenschutz-Compliance an diesen ausgerichtet haben. Der europäische Datenschutz als Gesamtkonstrukt wird durch die Datenschutzgrundverordnung gestärkt werden und könnte zu signifikanten Wettbewerbsvorteilen für europäische Unternehmen speziell gegenüber den USA führen, da auch Unternehmen außerhalb Europas an das EU-Recht gebunden werden sollen, wenn sie auf Daten von EU-Bürgern zugreifen. Die Datenschutzverordnung kann in diesem Lichte somit als großer Chance für Europa gesehen werden.

Bei der Betrachtung möglicher Wertschöpfungspotentiale durch den Datenschutz muss jedenfalls eine Einzelbewertung vorgenommen werden, da diese nicht bei jedem Unternehmen in gleicher Form vorliegen. Kosteneffizientes Implementieren eines CMS sollte die Grundvoraussetzung darstellen und von jedem Unternehmen innerhalb der gesetzlichen Bestimmungen durchgeführt werden. Neben der Minimierung der Kosten besteht für manche Unternehmen unter bestimmten

Bedingungen die Möglichkeit, den Datenschutz als Instrument zur aktiven Wertschöpfung zu nutzen. Diese Möglichkeit setzt voraus, dass der Datenschutz aus Kundensicht einen entscheidenden Faktor für die Wahl des betrachteten Unternehmens darstellt. Liegen in weiterer Folge die Kundenerwartungen über den gesetzlichen Bestimmungen und den Regelungen der Konkurrenzunternehmen, besteht die Möglichkeit, den Datenschutz als Alleinstellungsmerkmal zu nutzen. Der Datenschutz kann somit unter bestimmten Voraussetzungen nicht nur als Hemmschuh, sondern durchaus als wertschöpfender Faktor angesehen werden. Dies gilt sowohl für einzelne Unternehmen als auch aus Sicht einer gesamteuropäischen Einheit, da ein durch die Datenschutzgrundverordnung gestärkter europäischer Datenschutz ein großer Vorteil im globalen Konkurrenzkampf sein kann.

Allgemein betrachtet kann somit festgehalten werden, dass der europäische Datenschutz vor allem langfristig gesehen wertschöpfenden Nutzen entfalten kann. Vor dem Hintergrund des gesellschaftlichen Wandels und des steigenden Bewusstseins um den Wert von Daten ist es Unternehmen anzuraten, sich intensiviert mit dem Thema Datenschutz auseinanderzusetzen und die Datenschutz-Compliance nicht als lästige Pflicht, sondern vielmehr als wirtschaftliche Chance wahrzunehmen.

Literaturverzeichnis

Agentur der Europäischen Union für Grundrechte: Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden, Luxemburg 2012, http://fra.europa.eu/sites/default/files/tk3109265dec_de_web.pdf, abgefragt am 29.5.2015

Becker, W./Urlich, P., Corporate Governance und Controlling – Begriffe und Wechselwirkungen. In: Keuper, F./Neumann, F. (Hrsg.): Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien, 1. Auflage, Wiesbaden 2010, S. 3-28

CERN: The birth of Web, http://home.web.cern.ch/topics/birth-web, abgefragt am 6.7.2015

Cochrane, P., In: Symantec, State of Privacy Report 2015, http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf, abgefragt am 20.6.2015

Europäische Kommission, Pressemitteilung: Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, http://europa.eu/rapid/press-release_IP-12-46_de.htm?locale=en, abgefragt am 22.6.2015

Gabler Wirtschaftslexikon, Stichwort: Wertschöpfung. In: Springer Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Archiv/54898/wertschoepfung-v8.html, abgefragt am 25.6.2015

Knyrim, R./Trieb, G., Das künftige EU-Datenschutzrecht - Neue Anforderungen an die betriebliche Compliance. In: Burger-Scheidlin, M. et al. (Hrsg.): Compliance Praxis, Ausgabe 2, Wien 2014, S. 30-33

Kroeber-Riel, W., Die betriebliche Wertschöpfung: Unter besonderer Berücksichtigung des Handels. In: Schnutenhaus, O. (Hrsg.): Vertriebswirtschaftliche Abhandlungen des Instituts für industrielle Verbrauchsforschung und Vertriebsmethoden an der Technischen Universität Berlin, Heft 6, Berlin 1963

von Lieven, S., Kommentar: EU-Datenschutz-Grundverordnung – Chance oder Risiko? In: Artegic Blog, https://www.artegic.de/eCRM/artegic-ECRM-DE/Aktuelles_Kommentar:.EU-Datenschutz-Grundverordnung...Chance.oder.Risiko._0cq-5gr.html, abgefragt am 20.6.2015

Moosmayer, K.: Compliance – Praxisleitfaden für Unternehmen, 2. Auflage, München 2012

Muth, T., Erfolgsfaktor Compliance-Kultur. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 205-238

Richter, F., Dialog: Datenschutz als Wettbewerbsvorteil . vielleicht klappt es doch… In: Berliner Datenschutzrunde: Initiative für einen modernen Datenschutz, https://www.berliner-datenschutzrunde.de/node/177, abgefragt am 28.6.2015

Rohde-Liebenau, B., Compliance² – einfache Antworten auf neue Anforderungen. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 37-55

Schließmann, C., Compliance im Kontext internationaler Strukturen, Geschäftsmodelle und Wertschöpfungsprozesse. In: Berufsverband der Compliance Manager (Hrsg.): Compliance 2015: Perspektiven einer Entwicklung, 1. Auflage, Berlin 2015, S. 141-162

Symantec, State of Privacy Report 2015, http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf, abgefragt am 20.6.2015

Ufer, F., Blog: Big Data: Ist Deutschland international wettbewerbsfähig? In: Big Data Blog 2015, https://bigdatablog.de/2015/02/19/big-data-ist-deutschland-international-wettbewerbsfaehig/, abgefragt am 20.6.2015

Youyou, W./Kosinski, M./Stillwell, D., Studie: Computer-based personality judgements are more accurate than those made by humans, http://www.pnas.org/content/112/4/1036.full, abgefragt am 6.7.2015

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs	Absatz
Art	Artikel
CMS	Compliance Management System
EU	Europäische Union
EU-DS-GVO	EU-Datenschutz-Grundverordnung
FTP	File Transfer Protocol
GVO-E	Grundverordnungs-Entwurf
S	Satz
USP	Unique Selling Point
US	United States
USA	United States of America