HWZ Hochschule für Wirtschaft Zürich

Zertifikatsarbeit CAS Digital Risk Management

# Big Data - Chancen und Risiken für Schweizer Unternehmen


**Eingereicht durch:**

Nadine Gloor

Bahnhofstrasse 122

8620 Wetzikon

**Eingereicht bei:**

Manuel P. Nappo, lic. Oec. HSG
Studienleiter MAS Digital Business

Ralph Hutter
Studienleiter CAS Digital Risk Management

Abgabetermin: 18. Juni 2016

# I. Management Summary

**Fragestellung.** Bereits heute sind alle jungen Schweizerinnen und Schweizer online vernetzt und hinterlassen eine Datenspur. Diese sogenannten Big Data können von Unternehmen oder Staaten gesammelt und ausgewertet werden. Dies ist ein relativ neues Geschäftsmodell, weshalb viele offene Fragen bis heute unbeantwortet bleiben. Deshalb beschäftigt sich die Autorin mit der Fragestellung: „Welches sind die Chancen und Risiken von Schweizer Unternehmen bei der Nutzung von Big Data?“

**Aufbau.** Zuerst wurde die Frage beantwortet, was Big Data genau ist. Hier stellte sich heraus, dass das Thema Datenschutz oft als Risiko erwähnt wird. Deshalb folgt ein Exkurs ins Thema Datenschutz in der Schweiz sowie in Europa und den USA. Danach wurden Chancen und Risiken von Big Data recherchiert und aufgeführt. Es wurde primär Literaturrecherche respektive Online-Recherche betrieben.

**Datenschutz.** Die Datenschutzgesetze sind noch nicht auf die Anforderungen von Big Data eingestellt. Die neue EU-Datenschutz-Grundverordnung, die 2018 in Kraft tritt, bringt einige Anpassungen, besonders für die Zusammenarbeit über die Staatsgrenzen hinweg. Die Schweizerische Gesetzgebung wird sich dieser Verordnung annähern müssen. Eine Neuerung wird sein, dass US-Unternehmen stärker in die Pflicht genommen werden und hohe Bussen bei Nichterfüllung erhalten können. In Bezug auf Big Data sollen pseudonymisierte Daten die Lösung bringen. Das Problem sind jedoch Persönlichkeitsprofile, bei denen anonymisierte respektive pseudonymisierte Daten verknüpft werden und so trotzdem auf eine bestimmte Person hinweisen. Es gibt verschiedene Ansätze, wie der Datenschutz angepasst werden könnte.

**Chancen und Risiken.** Für Marketing und Werbung birgt die datenbasierte Zielgruppenansprache ein enormes Potential. Wohingegen für die User das Phänomen „Filter Bubble“ droht. Technologie ist die Basis für Big Data. Bis jetzt fehlen standardisierte Systeme. Hier drohen Cyber-Attacken, die auch in der Schweiz vermehrt auftreten. Sogenannte Künstliche Intelligenzen sollen beim Auswerten der Daten helfen, diese sind jedoch noch Zukunftsmusik. Eine Quelle für Big Data ist das Internet of Things, das Gegenstände online verknüpft. Grosse Firmen oder Staaten besitzen die Mittel, um die Datenmengen auszuwerten. Im Gegensatz zu einfachen Bürgern. So bilden sich Datenmonopole. Big Data kann verwendet werden, um Prognosen aufzustellen. Diese können hilfreich sein, sind jedoch immer vergangenheitsorientiert.

**Ausblick.** Die Auswertung von grossen Datenmengen ist für viele Branchen attraktiv. Heute fehlen noch die technischen Voraussetzungen und die Gesetzeslage ist unklar. Vieles deutet jedoch daraufhin, dass diese Thematik bereits in den Startlöchern steht. Der Staat und die Unternehmen sowie die Gesellschaft müssen sich der Risiken bewusst sein und sie diskutieren.

# II. Erklärung

Hiermit erkläre ich, die vorliegende Arbeit selbstständig und nur unter Benutzung der angegebenen Hilfsmittel und Literatur verfasst zu haben.

Nadine Gloor
Wetzikon, 18. Juni 2016

# Inhaltsverzeichnis



# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1. Einleitung

## 1.1. Ausgangslage

*„We are drowning in data but starving for knowledge“* (John Naisbitt,1984).

Am 21.03.2016 um 16.53 Uhr betrug die Grösse des Internettraffics in einer Sekunde 33‘753 GB weltweit. Ausserdem wurden 7150 Tweets abgeschickt, 488 Fotos bei Instagram hochgeladen, 2066 Telefonanrufe über Skype getätigt, 53‘424 Google Suchen gestartet, 119‘187 YouTube Videos angeschaut und 2‘475‘857 E-Mails verschickt. Zu diesem Zeitpunkt gab es zudem 1‘004‘602‘236 Websites (Internet live stats, 2016).

Eine Studie aus dem Jahr 2014 sagte schon voraus, dass es 2016 weltweit über 2 Milliarden Smartphone User haben würde. 2018 sollen über 50% der Mobiltelefone Smartphones sein (eMarketer, 2014).

Abbildung 1 zeigt den Anstieg der Internetnutzung der Schweizer Bevölkerung. Besonders die mobile Nutzung hat in den letzten Jahren stark zugenommen. Zu beachten ist, dass auch zu Hause mit einem mobilen Gerät wie einem Smartphone oder Tablet aufs Internet zugegriffen werden kann. „Mobil“ heisst also nicht automatisch „unterwegs“ (Bundesamt für Statistik, 2016a).

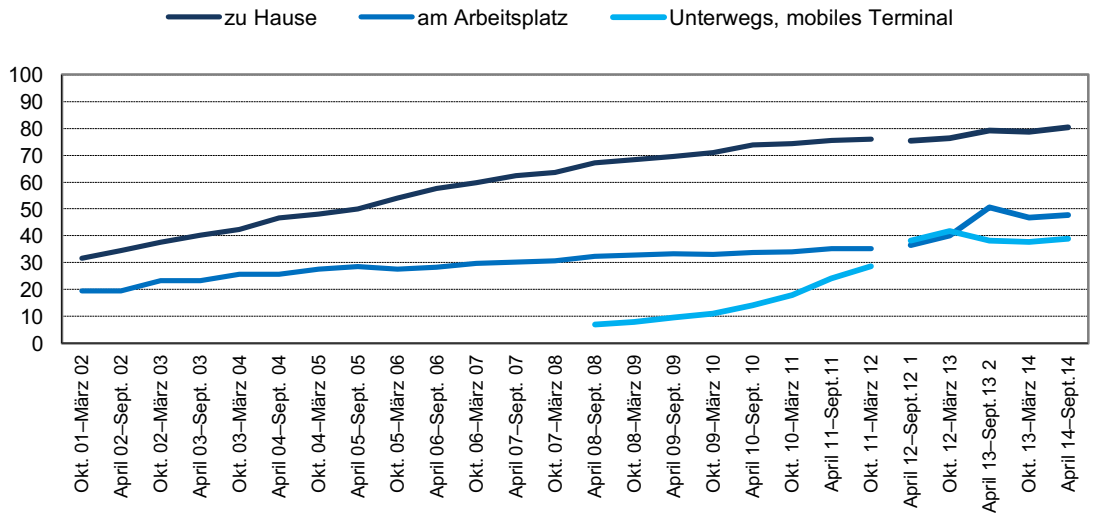


**Abbildung 1:** Internetnutzung der Schweizer Bevölkerung (Bundesamt für Statistik, 2016a)

In der OECD gibt es einen relativ grossen „Digital Divide“ – 49% der 65- bis 74-jährigen nutzten 2014 das Internet, im Gegensatz zu 95% der 16 bis 24-Jährigen. In der Schweiz sind über 60% der älteren Generation online und 100% der Jungen. Besonders die Jungen von heute respektive die Erwachsenen von Morgen hinterlassen intensiv Daten im Web (OECD, 2015, S. 52).

Die Menge an Daten, welche die Menschen heutzutage im Internet veröffentlichen ist immens. Vor allem dank Smartphones wird immer und überall eine Datenspur hinterlassen. Diese Daten sagen einiges aus über die Interessen, das Kaufverhalten oder die Persönlichkeit einer Person. Unternehmen können diese Daten nutzen, beispielsweise für personalisierte Werbung. Doch Daten zu haben, heisst noch nicht, sie auch nutzen zu können. Dazu müssen sie zuerst ausgewertet werden. Hier kommt zudem der Daten- und Persönlichkeitsschutz zum Tragen. Diese Themen sollen in dieser Arbeit für den CAS Digital Risk Management an der Hochschule für Wirtschaft in Zürich behandelt werden.

## 1.2. Fragestellung und Abgrenzung

Viele Unternehmen wissen einerseits nicht, welche Chancen sich bieten durch diese Datenmenge. Andererseits sind sie sich der Risiken nicht bewusst. Diese Arbeit soll einen Überblick über die Chancen und Risiken von Big Data für Schweizer Unternehmen bieten. Zudem soll ein Blick in die Datenschutz Gesetzeslage in der Schweiz geworfen werden. Die Fragestellung lautet somit folgendermassen:

> *Welches sind die Chancen und Risiken von Schweizer Unternehmen bei der Nutzung von Big Data?*

In dieser Arbeit wird kein konkretes technisches Vorgehen beschrieben, wie diese Massnahmen umgesetzt werden können. Auch beschränkt sich die Autorin nicht auf eine spezifische technische Lösung.

## 1.3. Aufbau und Methodik

Zuerst wird definiert, was Big Data genau ist und verschiedene Quellen zum Thema werden analysiert. Zudem wird ein Exkurs in die Daten- und Persönlichkeitsschutzrichtlinien der Schweiz gemacht. Der Fokus liegt auf der Schweiz, da das Internet jedoch keine Landesgrenzen kennt, wird auch der Einfluss auf und vom Ausland betrachtet. Dieses Kapitel basiert auf Literaturrecherche.

Anschliessend werden verschiedene Anwendungsfälle von Big Data aufgezeigt und deren Chancen und Risiken näher betrachtet.

Zum Schluss werden die Erkenntnisse aus der Recherche zusammengefasst.

# 2. Theoretische Grundlagen

## 2.1. Big Data

„Big Data“ bezeichnet die enorme Menge an Daten, die durch die Nutzung von Internet, Smartphones, soziale Medien, aber auch durch die Verwendung von Kredit- und Kundenkarten oder Überwachungskameras entstehen, gesammelt und ausgewertet werden. Durch diese Auswertung können Unternehmen oder Organisationen beispielsweise Einblick in das Verhalten ihrer Kundinnen und Kunden gewinnen. Dadurch kann gezieltes Marketing und Verkaufsförderung betrieben werden. Die grosse Herausforderung ist nach wie vor der Daten- und Persönlichkeitsschutz. Oft gibt der User keine explizite Erlaubnis, dass seine Daten in dieser Art und Weise benutzt werden dürfen (Springer Gabler Verlag, 2016a).

Um die grossen Daten auszuwerten, wird sogenanntes „Data Mining“ betrieben. Beispielsweise werden Algorithmen verwendet, um aus den rohen Daten Zusammenhänge herzustellen. Denn die Rohdaten an sich nützen den Unternehmen wenig. Die Herausforderung bei Data Mining ist, dass das System nach Interessantheit und Nützlichkeit filtern können muss. Eine reine statistische Auswertung ist nicht ausreichend bei solchen Datenmengen (Springer Gabler Verlag, 2016b).

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) definiert Big Data so:

*„Grosse Datenmenge aus vielfältigen Quellen, die mit hoher Verarbeitungsgeschwindigkeit erfasst, gespeichert und für unbestimmte Zwecke auf unbestimmte Zeit für Auswertungen und Analysen verfügbar gemacht werden“ (EDÖB, 2016a).*

Big Data definiert sich durch die fünf Vs, welche auch die grössten Herausforderungen im Zusammenhang mit Big Data beschreiben (Cheesman, 2016):

- **V**olume: Big Data besteht, wie der Name schon sagt, aus einer enormen Masse aus Daten. Die Herausforderung ist, diese Masse überhaupt bearbeiten zu können.
- **V**elocity: Die Daten sind nicht nur gross, sondern auch enorm schnell. Sie entstehen rapide und verbreiten sich innert Sekunden um den ganzen Planeten.
- **V**ariety: 80% aller Daten ist unstrukturiert und es gibt unzählige Variationen von Daten.
- **V**eracity: Sind die Daten, welche gesammelt wurden überhaupt richtig und relevant?
- **V**alue: Der letzte und wohl wichtigste Punkt. Es ist essentiell zu wissen, welche Daten wie viel wert sind und welche sich somit zu Sammeln lohnt.

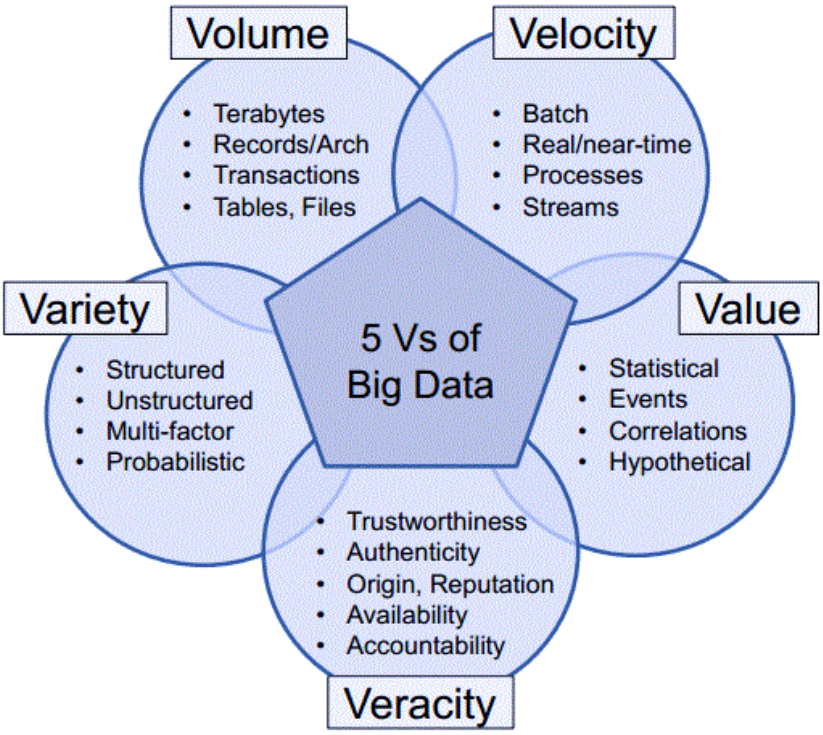


**Abbildung 2:** Die 5 V's von Big Data (Cheesman, 2016)

Eine essentielle Fragestellung bei Big Data ist der Datenschutz. Auf dieses Thema wird im nächsten Kapitel genauer eingegangen.

Eckert beschreibt eine Value Chain für Big Data, die aus folgenden fünf Schritten besteht (2016, Folie 51). Alle Schritte gelten als „Datenbearbeitung".

1. Sammeln (datacollection)
2. Speichern (storage)
3. Zusammenführen (aggregation)
4. Auswertung und Datenanalyse (analysis)
5. Verwertung (use of results)

## 2.2. Exkurs Datenschutz

Da im Zusammenhang mit Big Data immer auch die Probleme mit dem Datenschutz angesprochen werden, soll dieses Kapitel einen Überblick über den aktuellen gesetzlichen Stand geben. Zuerst wird das Datenschutzgesetz in der Schweiz betrachtet, anschliessend die Gesetzeslage in der EU und der USA. Zudem wird auf Allgemeine Geschäftsbedingungen (AGB) und Datenschutzerklärungen eingegangen.

### 2.2.1. Datenschutzgesetz der Schweiz

> *„Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden“ (DSG, 2015, Art. 1).*

Wie Artikel 1 bereits sagt, schützt das Schweizerische Datenschutzgesetze (DSG) nicht die Daten an sich, sondern die Person, die hinter den Daten steht. Der Schutz der Privatsphäre einer Person ist auch in der Bundesverfassung der Schweizerischen Eidgenossenschaft als Grundrecht in Artikel 13 festgelegt. Dort heisst es, dass jede Person „Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs“ hat. Zudem hat jeder und jede „Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten“ (Bundesverfassung der Schweizerischen Eidgenossenschaft, 2016, Art. 13).

Das DSG bezieht sich primär auf nicht anonymisierte Personendaten. Dies sind Daten, die sich auf eine bestimmbare Person beziehen. Dies sind Angaben wie Name, Alter, Wohnort, aber auch die IP-Adresse oder die Gerätenummer. Ausserdem hebt das DSG Personendaten, die besonders schützenswert sind, hervor. Dies sind beispielsweise Daten über die religiöse Gesinnung einer Person, deren politische Meinung, Daten zum Gesundheitszustand, Rassenzugehörigkeit oder ob eine Person soziale Hilfe beansprucht. Werden verschiedene Daten zu einer Person zusammengestellt, entsteht ein sogenanntes Persönlichkeitsprofil. Dieses lässt bis zu einem gewissen Grad eine Beurteilung der betroffenen Person zu (DSG, 2014, Art. 3).

In Artikel 4 werden die Grundsätze für die Bearbeitung von Daten beschrieben (ebd.):

- **Rechtmässigkeit**: Wenn jemand Personendaten bearbeiten will, braucht er oder sie einen sogenannten Rechtfertigungsgrund. Auf diese wird nachfolgend genauer eingegangen.
- **Verhältnismässigkeit**: Die Bearbeitung soll nach „Treu und Glauben“ geschehen und „verhältnismässig“ sein. Der Datenschutzbeauftragte des Kantons Zürich Bruno Baeriswyl drückte es im Unterricht zum CAS Digital Risk Managment an der HWZ, folgendermassen aus: „So wenig wie möglich, so viel wie nötig“.
- **Zweckbindung**: Die gesammelten Daten dürfen nur für denjenigen Zweck bearbeitet werden, der für die betroffene Person bei der Erhebung ersichtlich war. Das heisst, dass ein Datensammler immer deutlich angeben muss, für welchen Zweck die Daten gesammelt werden. Das bedeutet, dass sich der Sammler im Klaren darüber sein muss, für was er die Daten in Zukunft brauchen wird.
- **Erkennbarkeit**: Dieser Punkt knüpft an den Vorherigen an. Die betroffene Person muss klar erkennen können, dass ihre Daten gesammelt werden und für welchen Zweck dies geschieht.

- **Einwilligung**: Muss die betroffene Person zur Datensammlung einwilligen, ist diese Einwilligung nur gültig, wenn die Person die Möglichkeit hatte, sich ausreichend zu informieren. Ausserdem muss die Einwilligung freiwillig geschehen. Bei besonders schützenswerten Personendaten oder bei Persönlichkeitsprofilen muss eine ausdrückliche Einwilligung vorliegen.

Artikel 13 beschreibt die Gründe, die eine Sammlung und Bearbeitung von Daten ohne die Einwilligung der betroffenen Person rechtfertigen. Ohne Rechtfertigung und Einwilligung ist es eine Verletzung der Persönlichkeit und somit widerrechtlich. Grundsätzlich gilt, dass entweder ein überwiegendes privates oder öffentliches Interesse bestehen muss oder ein Gesetz die Sammlung rechtfertigt. Folgende Punkte können als überwiegendes Interesse der datenbearbeitenden Person oder des Unternehmens gewertet werden (DSG, 2014):

- Im Zusammenhang mit einem **Vertragsabschluss**,
- bei **wirtschaftlichem Wettbewerb**,
- zur Prüfung der **Kreditwürdigkeit** in Zusammenhang mit einem Vertragsabschluss (unter Ausschluss von besonders schützenswerten Personendaten und Persönlichkeitsprofilen),
- bei der Veröffentlichung von beruflichen Personendaten in **redaktionellen Medien**,
- für nicht personenbezogenen Zwecken in **Forschung, Planung und Statistik**,
- und bei **Personen des öffentlichen Lebens** in Bezug auf eben dieses.

Die Person oder das Unternehmen, welche Daten sammelt, muss sicherstellen, dass die Daten sicher vor Angriffen resp. Diebstahl sind. Das DSG erwähnt in Artikel 7 „angemessene technische und organisatorische Massnahmen“, um die Daten zu schützen. Diese Massnahmen werden im Anhang zu den Richtlinien über die Mindestanforderungen von Datenschutzmanagementsystemen definiert (2010, Ziffer g). Die Umsetzung diese Punkte stützt sich auf Anhang A der ISO Norm 27002. Da die genaue Analyse dieser ISO Norm den Rahmen dieser Arbeit sprengen würde, wird nicht näher darauf eingegangen.

- **Datenvertraulichkeit**: Personendaten dürfen nicht von unbefugten Personen, Stellen oder Prozessen, aufgerufen werden können.
- **Datenintegrität**: Es muss sichergestellt werden, dass die Personendaten vollständig und aktuell sind. Die betroffene Person darf jederzeit Verlangen, dass falsche Daten berichtigt werden (DSG, 2014, Art. 5).
- **Datenverfügbarkeit**: Jede Person darf jederzeit Einsicht in ihre Daten verlangen. Deshalb müssen die Daten immer zu Verfügung stehen (ebd., Art. 8). Eine Einschränkung dieser Auskunftspflicht gilt nur bei überwiegendem Interesse des Datenbankinhabers (ebd., Art. 9).

- **Datenbearbeitung durch Dritte**: Werden die Daten an ein Drittunternehmen zur Bearbeitung weitergegeben, muss auch dieser die Datensicherheit gewährleisten. Laut Artikel 10a, darf der Dritte die Daten nur so bearbeiten, wie es der Auftraggeber selbst hätte tun dürfen (DSG, 2014).

Gehen Personendaten unbeabsichtigt verloren oder werden gestohlen, ist dies meist auf eine Verletzung des DSG Artikel 7 zurückzuführen. Das Schweizerische Gesetz verpflichtet in so einem Fall nicht zwingend zur Information des EDÖB oder der betroffenen Personen. Allerdings lässt sich laut Vasella (2015, S. 291) aus dem Grundsatz von Treu und Glaube (UWG, 2014, Art. 2), aus Artikel 7 (DSG, 2014) und allfälligen ABG ableiten, dass die vom Leck betroffenen Personen und User informiert werden sollen.

### 2.2.2. Datenschutz im Ausland

Das DSG regelt auch die Datenbekanntgabe über die Schweizer Grenzen hinweg. In Artikel 6 (ebd., 2014) wird beschrieben, unter welchen Umständen Daten ins Ausland geschickt werden dürfen. Grundsätzlich gilt, dass das Land, in das die Daten übertragen werden, „angemessenen Schutz" bieten muss. Ohne einen solchen Schutz müssen folgende Punkte erfüllt werden:

- Mittels Vertragsabschluss wurde garantiert, dass die Daten auch im Ausland geschützt werden.
- Die betroffene Person hat der Übertragung ins Ausland eingewilligt.
- Die Daten werden im Zusammenhang mit einem Vertragsabschluss übertragen.
- Wenn die „Wahrung eines überwiegenden öffentlichen Interesses" (ebd., Art. 6) die Übertragung unerlässlich macht. Dies gilt auch für Daten im Zusammenhang eines Gerichtsfalls.
- Der Schutz des Lebens oder der Gesundheit einer Person hängt von der Bekanntgabe der Daten ab.
- Die Daten wurden von der betroffenen Person öffentlich zugänglich gemacht. Die Verordnung zum DSG ergänzt in Artikel 5 (2014) folgendes: „Werden Personendaten mittels automatisierter Informations- und Kommunikationsdienste zwecks Information der Öffentlichkeit allgemein zugänglich gemacht, so gilt dies nicht als Übermittlung ins Ausland". Dies trifft beispielsweise auf persönliche Profile im Web oder auf Social Media Plattformen zu.

Wenn ein Unternehmen unter internationaler Leitung steht, dürfen Daten über die Landesgrenzen hinweg ausgetauscht werden. Die Bedingung ist jedoch, dass alle Beteiligten angemessenen Datenschutz gewährleisten (ebd., Art 6).

Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) veröffentlicht eine Liste mit der Übersicht über den Stand des Datenschutzes in den einzelnen Ländern. Dort ist auch zu entnehmen, dass beispielsweise die USA einen ungenügenden Schutz bietet, die meisten europäischen Länder jedoch schon (EDÖB, 2016b, S. 1-11).

**Europa**

Im Dezember 2015 hat sich die Europäische Kommission, der Europäische Rat und das Europäische Parlament über den finalen Inhalt der neuen „EU-Datenschutz-Grundverordnung“ (DSGVO) geeinigt. Voraussichtlich wird die neue Verordnung 2018 in Kraft treten. Sie wird die bis jetzt geltende EU-Datenschutzrichtlinie von 1995 ersetzen. Der grösste Unterschied zwischen 1995 und heute ist die Digitalisierung. Deshalb fokussiert sich die neue Verordnung auf dieses Thema. Dies sind die wichtigsten Neuerungen (Datenschutzbeauftragter, 2015):

- **Vereinheitlichung:** Mit der neuen DSGVO soll der Datenschutz unter den EU-Staaten vereinheitlicht werden.
- **Nutzerrechte werden gestärkt**: Der Zugang zu den eigenen Daten soll vereinfacht und die Transparenz erhöht werden. Zudem sollen die User die Möglichkeit haben, ihre Daten von einer Plattform zu einer anderen zu transportieren. Dies, weil die Daten dem User gehören und nicht der Plattform, welche sie gesammelt hat. Auch soll der User ein „Recht auf Vergessen“ erhalten und „Privacy by Default / Design“ soll zum Standard werden.
- **Mindestalter wird erhöht:** Neu soll das Mindestalter für die rechtwirksame Einwilligung zum Sammeln und Bearbeiten von Personendaten von 13 auf 16 Jahre erhöht werden.
- **US-Unternehmen werden an das EU-Recht gebunden:** Nicht nur EU-Unternehmen, sondern auch spezifisch US-Unternehmen, müssen sich an die neuen Regeln halten.
- **Hohe Bussgelder:** Neu können bei Verstössen Bussgelder von bis zu 4 Prozent des Jahresumsatzes eines Unternehmens verlangt werden.

Kasack (2015) sieht zwei Seiten der neuen Verordnung. Einerseits schreibt er, dass vielen Internet-Usern nicht klar ist, was Internet Konzerne wie Facebook und Co. mit ihren Daten machen dürfen. Sie geben freiwillig persönliche Daten preis und akzeptieren die Allgemeinen Geschäftsbedingungen (AGB) immer wieder von neuem. Das Problem sind die fehlenden Alternativen. Denn wer die AGB nicht akzeptieren will, muss als Konsequenz sein Konto löschen. Doch was ist die Alternative zu Google, Instagram, Pinterest usw.? Andererseits meint Kasack, dass die User den Wert ihrer Daten nicht einschätzen können. Viele Internetdienste funktionieren „auf der Basis Dienstleistung gegen Daten“. Nicht umsonst spricht man davon, dass Daten das „Öl des 21. Jahrhunderts“ sind. Doch der Ölpreis ist bekannt, derjenige von Daten nicht.

Um den Umgang mit Big Data zu erleichtern, soll im Rahmen der DSGVO eine sogenannte Pseudonymisierung eingeführt werden. Pseudonymisierte Daten sind solche, die nicht mehr einer eindeutigen Person zugeordnet werden, aber dennoch miteinander verknüpft werden können. Pseudonymisierte Daten sind jedoch keine vollständig anonymisierten Daten – deshalb gelten sie eigentlich als Personendaten. Die Frage ist nun, ob die Neuerung trotzdem ausreichend ist für die Möglichkeiten, die Big Data bietet (BR News, 2016).

Ein weiterer wichtiger Punkt ist die explizite Einwilligung des Users, die mit der neuen Verordnung Pflicht wird. Das bedeutet, dass der User z.B. eine Box anklicken muss, um zu bestätigen,

dass er den AGB und den Datenschutzrichtlinien zustimmt. Die Box darf in Zukunft nicht mehr vorangewählt sein (ebd.).

Für die Schweiz ist es wichtig, dass das DSG dem DSGVO weitgehend angepasst wird. Denn nur so wird die Schweiz von der EU als genügend sicher betrachtet. Dies ist zentral für Schweizer Unternehmen, die Daten mit Unternehmen in der EU austauschen (Dr. Widmer & Partner – Rechtsanwälte, 2015).

**USA**

Wie in der Einleitung erwähnt, haben die USA keine angemessenen Datenschutzrichtlinien. Dies ist deshalb ein Problem, da enorm viele webbasierte Dienste aus der USA kommen; Facebook, Google, Twitter, Instagram, Amazon, ebay, Yahoo, LinkedIn usw.

Deshalb wurde zwischen der Schweiz und der USA das sogenannte „Safe Harbor" Abkommen unterzeichnet. Dies ist ein Regelwerk, „welches für die darunter zertifizierten Unternehmen ein ausreichendes Datenschutzniveau gewährleistet. Auf diese Weise wird der Datentransfer zwischen Schweizer und zertifizierten U.S. Unternehmen erheblich erleichtert." US-Unternehmen können sich beim Handelsministerium der USA zertifizieren lassen und gelten anschliessend als sicher genug, um einen Datenaustausch zu rechtfertigen (EDÖB, 2008/2009).

Am 6. Oktober 2015 hat der Europäische Gerichtshof dieses Abkommen jedoch für ungültig erklärt. Die Schweiz hat Interesse daran, ein neues Abkommen mittels einem „international koordinierten Vorgehen", also gemeinsam mit der EU, anzugehen. In der Zwischenzeit rät der EDÖB zu Vorsicht, wenn Daten mit der USA ausgetauscht werden. Dies bezieht sich auch auf die Verwendung diverser Online-Tools, welche aus der USA stammen oder dort betrieben werden, was für Schweizer Unternehmen einige Geschäftsprozesse verkompliziert (EDÖB, 2015a).

Bis zu einem neuen Abkommen, sollten Schweizer Unternehmen wieder vertragliche Garantien, wie in Artikel 6 im DSG (2014) festgehalten, aufsetzen, wenn sie Daten mit der USA austauschen möchten. Der EDÖB betont, dass folgende zwei Punkte dabei beachtet werden müssen (EDÖB, 2015b):

1. Die vom Datenaustausch betroffenen Personen müssen klar über die möglichen Risiken informiert werden.
2. Die betroffene Person muss von beiden Parteien beim Rechtsschutz unterstützt werden. Entsprechende Verfahren werden durchgeführt und allfällige Gerichtsurteile müssen akzeptiert werden.

### 2.2.3. Allgemeine Geschäftsbedingungen und Datenschutzerklärungen

Eigentlich gehören Datenschutzbestimmungen nicht in die Allgemeinen Geschäftsbedingungen (AGB), sondern in eine eigenständige Datenschutzerklärung. Laut Vasella (2015) können solche Bestimmungen in den AGB als „überraschend und daher ggf. unwirksam angesehen werden." Natürlich lohnen sich gegenseitige Verweise. Oft finden sich jedoch trotzdem Datenschutzbestimmungen in den AGB, weshalb in diesem Kapitel die Datenschutzrichtlinien jeweils ebenfalls mitgemeint sind (S. 272).

AGB gelten nur, wenn sie „verbindlich akzeptiert wurden" (ebd., S. 272). Das bedeutet, dass vor dem Abschluss z.B. eines Vertrags, deutlich auf die AGBs hingewiesen werden muss und dass der User ihnen zustimmt. Ausserdem müssen sie einfach auffindbar, lesbar und speicherbar sein. Im Web und besonders bei Social Media gilt global die sogenannte „Ungewöhnlichkeitsregel", die besagt, dass keine ungewöhnlichen Datenbearbeitungen vorgenommen werden dürfen. Falls doch, muss in den AGB der Hinweis hervorgehoben werden (z.B. grössere Schriftart, farblich markiert usw.) (ebd., S. 272-273).

AGB müssen verständlich sein. Das betrifft die Schriftgrösse, die Sprache und den Inhalt. Besonders bei sehr grossen AGB ist dies stets eine Gratwanderung. Sie dürfen nicht zu gross, aber auch nicht zu knapp ausfallen. Ein Mittelweg ist gefragt. Die AGB müssen in allen jenen Sprachen verfügbar sein, in denen die Plattform oder Website aufrufbar ist (ebd., S. 274).

Werden Änderungen in den AGB vorgenommen, muss nach Schweizer Recht aktiv und unübersehbar darauf hingewiesen werden. Der Hinweis, der User müsse sich regelmässig selbst über Änderungen informieren, ist nicht gültig (ebd., S. 275).

Zusammengefasst kann gesagt werden, dass ABG und Datenschutzerklärungen folgende Anforderungen erfüllen müssen (ebd., 277-278):

- Die Zustimmung muss vor der Registrierung oder dem Vertragsabschluss ausdrücklich erfolgen (z.B. mit einem Klick).
- Die AGB müssen leicht zugänglich sein.
- Der Inhalt, die Sprache und die Gliederung müssen so einfach wie möglich gestaltet sein. Keine Mehrdeutigkeiten.
- Datenbeschaffung, -bearbeitung und –bekanntgaben sind zu unterscheiden.
- Ggf. ungewöhnliche Bearbeitungszwecke müssen hervorgehoben werden.
- Ein Kündigungsrecht seitens des Plattformen- oder Webseitenbetreibers soll verankert sein. Dies kommt dann zum Zuge, wenn ein User den AGB nicht zustimmt.
- Bei Änderungen und Anpassungen muss der User aktiv informiert werden.

### 2.2.4. Big Data und Datenschutz

Eine grundsätzliche Frage, die sich beim Thema Big Data stellt, ist die des Datenschutzes. Datenschutzgesetze schützen, wie in diesem Kapitel erwähnt, primär Personendaten. Häufig wird argumentiert, dass bei Big Data nur anonyme Daten oder sogenannte „reine Sachdaten" gesammelt werden und somit der Datenschutz nicht greift (EDÖB, 2016a). Allerdings kann nicht ausgeschlossen werden, dass beim Zusammenführen von mehreren einzelnen Datensträngen evtl. eine Identifikation möglich wird. Das zeigt beispielsweise eine Studie aus dem Jahr 1990 von Latanya Sweeney, einer Professorin an der Harvard University. Sie besagt, dass 87% aller Amerikanerinnen und Amerikaner mit nur drei Angaben eindeutig identifiziert werden können: Postleitzahl (ZIP-Zahl), Geschlecht und Geburtsdatum (ebd., 2000).

Zudem ist laut EDÖB auch die weitere technische Entwicklung ein Unsicherheitsfaktor (2016a):

> *„Was heute als „anonym" gilt, kann morgen eventuell aufgrund des rapiden technologischen Fortschritts und zusätzlicher Datenquellen ohne grossen Aufwand einer bestimmten Person zugeordnet werden und so möglicherweise eine grobe Persönlichkeitsverletzung darstellen."*

Deshalb wird dafür plädiert, dass die Grundsätze des Datenschutzes bereits bei der Entwicklung neuer Technologien miteinbezogen wird, beispielsweise mit dem Konzept „Privacy by Default / Design" (EDÖB, 2016a).

# 3. Chancen und Risiken

Dieses Kapitel behandelt mögliche Chancen und Risiken, die der Umgang mit Big Data mit sich bringt. Da bekanntlich aus Risiken Chancen werden können, kann keine gerade Linie zwischen Risiko und Chance gezogen werden.

Eine Studie der Berner Fachhochschule im Auftrag des Bundesamts für Kommunikation aus dem Jahr 2015 (Prof. Dr. Jarchow und Estermann, 2015) hat 20 Experten aus Wirtschaft, Verwaltung sowie der Gesellschaft qualitativ und 800 Schweizer Individuen quantitativ zum Thema „Chancen und Risiken von Big Data" befragt. Die in dieser Studie meistgenannten Chancen und Risiken sind in der nachfolgenden Tabelle zusammengefasst (S. 13-17). Danach werden einige dieser Risiken und Chancen näher betrachtet.

**Tabelle 1:** Chancen und Risiken von Big Data (Prof. Dr. Jarchow und Estermann, 2015)

| Big Data | Nr. | Beschreibung |
|---|---|---|
| **Chancen** | 1 | Neue Erkenntnisse gewinnen und neue Zusammenhänge entdecken dank Kombination und Analyse der Daten. |
| | 2 | Personalisierung von Angeboten, Infos und Werbung. |
| | 3 | Verbesserte Prognosen in verschiedenen Bereichen. |
| | 4 | Mehr Agilität dank Echtzeit-Auswertungen. |
| | 5 | Vermehrt können faktenbasierte Entscheide getroffen werden. |
| **Risiken** | 6 | Datenschutzproblematik |
| | 7 | Image-Risiken bei Datenschutzverletzungen und dazugehörende Manipulationsgefahr. |
| | 8 | Erhöhte Kunden- resp. Auftragsgebererwartungen hinsichtlich datenbasierter Zusatzdienste. |
| | 9 | Fehlende Business-Cases für den rentablen Einsatz von Big Data, hohe Investitionen in Tools. Unternehmenskultur ist noch nicht bereit. |
| | 10 | Bedrohung der Privatsphäre |
| | 11 | Datenmonopole; Ungleichheit bei der Verfügung über die Daten, fehlender Datenzugang. |
| | 12 | Mangelndes Bewusstsein der User. |
| | 13 | Faktenbasierte Entscheide sind immer vergangenheitsorientiert – verdrängen unternehmerisches Gespür. |

**Marketing und Werbung** (Chance 2)

> „Noch nie waren so viele Daten über Zielgruppen und Kunden speicher- und analysierbar wie heute. Das Potenzial für Marketingzwecke ist praktisch unerschöpflich“ (PC-Magazin, 2014)“

Doch die Nutzung von Big Data im Marketing birgt einige Risiken. Denn die User achten besser auf ihre persönlichen Daten. Durch sogenannte Opt-in Verfahren, kann die Einverständnis der User eingeholt werden (siehe auch Kapitel Datenschutz). Auch für kleine Unternehmen ist es wichtig, dass sie ihre Daten angemessen schützen (PC-Magazin, 2014).

Big Data verspricht Marketing-Fachleuten personalisierbare Werbung, also auf den User zugeschnittene Anzeigen. Eli Pariser beschreibt zum ersten Mal den „Filter Bubble“ und löst eine

grosse Diskussion aus. Pariser warnt davor, dass irgendwann die vom System errechneten Interessen nicht mehr von den ureigen entwickelten zu unterscheiden sind. Der User sieht nur noch, was seinem Suchprofil entspricht (Thiel, 2012). Dies kann auch dazu führen, dass ein User in seiner extremen Ansicht immer weiter bestärkt wird, da er durch die Personalisierung immer die gleiche Weltansicht zu sehen bekommt. Besonders bei Google, aber auch bei Social Media Plattformen wie Facebook, arbeitet ein Algorithmus im Hintergrund. Dieser bestimmt, was den User interessiert und zeigt ihm oder ihr nur noch das an (Zeier, 2016).

**Technologie** (Chancen 1, 5 und Risiko 9)
Big Data hängt stark mit der Technologie zusammen. Einerseits können Daten nur mittels Technik gesammelt, andererseits nur durch sie ausgewertet und genutzt werden. Ein Faktor ist z.B. die Entwicklung von technischen Lösungen, die den Datenschutz per Default anbieten. Diese beinhalten beispielsweise Schranken oder Barrieren, die verhindern, dass Daten untereinander verknüpft werden (Prof. Dr. Jarchow und Estermann, 2015, S. 21-22). Bis jetzt gibt es noch keine standardisierten Programme, die sich auch kleinere Unternehmen leisten können. Eine solche Lösung müsste idealerweise mit bestehenden Programmen kompatibel sein (z.B. mit Data-Warehouses). Experten gehen davon aus, dass in drei bis fünf Jahren solche Standardtools zu Verfügung stehen werden (ebd., S. 22).

Ein weiteres Risiko bei Big Data ist die Cyber-Kriminalität im Zusammenhang mit Datenabfluss. Im Rahmen einer Studie wurden 1700 IT-Entscheidungsträger und 3500 Angestellte aus 12 Ländern bezüglich Cyber-Kriminalität befragt. Dabei gaben 32% der Fachleute an, dass sie davon ausgehen, dass ihr Unternehmen innert der nächsten 90 Tage angegriffen werden wird. Und 31% geben zu, nicht genügend dafür gewappnet zu sein (Loy, 2016). 2014 sind bei KOBIK, der Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität, über 10'000 Verdachtsmeldungen und Anfragen eingegangen. Das ist im Vergleich zu 2013 ein anstieg von 10.9%. Einerseits ging es um Hacking und DDoS-Attacken (Distributed Denial of Service) aber auch um Betrugs-E-Mails usw. (Bundesamt für Polizei fedpol, 2015, S. 3). Bei 9.07% der Angriffe ging es um Datenbeschädigung (ebd., S. 9).

Um die Masse der Daten auswerten zu können, wäre eine Lösung intelligente Systeme, sogenannte künstliche Intelligenz. Dies sind lernfähige Algorithmen, denen beigebracht wird, Daten zu interpretieren und die sich selbst weiterentwickeln und dazulernen (ebd., S. 22). Die Gefahr ist, dass solche Systeme einen Kontrollverlust herbeiführen können. Denn das System weiss am Ende mehr als der menschliche Betreiber (ebd., S. 23). Schon 1956 wurde der Begriff „Künstliche Intelligenz“ oder kurz „KI“ geprägt und die Forscher meinten, bald sei ein solches Programm Realität. Bisher konnte das Versprechen nicht eingehalten werden. Heute jedoch sieht es so aus, als sei die KI in greifbarer Nähe. Forscher haben nun begonnen, dem Computer das Lernen beizubringen (sogenanntes Deep Learning). Sie füttern das Programm mit massenweise Daten und es vernetzt diese zu Informationen, ähnlich wie das menschliche Gehirn.

Wer also die meisten und besten Daten besitzt, hat eine Vorherrschaft bei der Entwicklung einer KI (Drösser, 2015). Momentan hat wohl der Suchmaschinenanbieter Google resp. der Mutterkonzern Alphabet die Nase vorne bei der Entwicklung von künstlicher Intelligenz. 2016 schlug eine KI von Google beim Spiel „Go" den menschlichen Meisterspieler aus Süd-Korea Lee Sedol vier zu eins. Kevin Kelly, Technologieexperte sagt in der FAZ:

> *„Google nutzt seine künstliche Intelligenz nicht vorrangig dafür, Suchanfragen besser zu beantworten. Es nutzt die Suchanfragen, um seine künstliche Intelligenz zu verbessern" (Schwägerl, 2016).*

Doch was tut der Mensch mit diesem Wissen aus der künstlichen Intelligenz? Wem gehört es? Die Manipulationsgefahr ist zudem gross, da Systeme noch immer von menschlichen Programmierern Befehle erhalten (Ebd., 2016).

Ein Feld, welches immer wichtiger wird, ist das Internet der Dinge (Internet of Things oder kurz IoT). Alltägliche Gegenstände, aber auch komplexe Industriemaschinen werden vernetzt und sammeln Daten. 2013 waren bereits neun Milliarden Geräte am Internet angeschlossen und untereinander verbunden. Bis 2020 sollen es 20 Milliarden sein, laut Robert Gebel, Chef der Geschäftsentwicklungsabteilung der Swisscom. Beispielsweise der Automobilhersteller Tesla sammelt rund 1.6 GB Daten pro Monat von jedem einzelnen Fahrzeug. Diese nutzen sie, um ihr Produkt schnell und wirksam weiter zu entwickeln. Doch nicht immer profitieren ausschliesslich die Nutzenden, sondern primär die Firmen (Sander, 2015).

Die Swisscom baut in der Schweiz ein eigenes Netz für das Internet of Things – das sogenannte Low Power Network (LPN). Dieses Netz ist geeignet für Geräte, die kleine Datenpakete untereinander übermitteln. Es benötigt wenig Energie und bietet eine kleine Bandbreite, gerade genug für das Internet der Dinge. Bei Autos oder in der Industrie werden die Daten wie bisher mittels Mobilfunknetz übertragen. Bis Ende 2016 will die Swisscom 80% der Schweizer Bevölkerung draussen an dieses Netz angeschlossen haben (Swisscom, 2016).

**Datenschutz** (Chance 1 und Risiko 6, 7 und 12)
Gerade beim Internet der Dinge stellt sich die Frage nach dem Datenschutz ganz besonders. Bei der Swisscom entscheidet beispielsweise ein „Ethik Board", ob eine Datenauswertung dem Datenschutz entspricht oder nicht (Sander, 2015). Auch beim Auto geht es um Bewegungsprofile oder um Unfall- resp. Gesundheitsdaten, die ggf. an die Versicherung weitergegeben werden können.

Der Schutz der Personendaten ist generell eines der grössten Risiken von Big Data. Die Frage ist, ob der traditionelle Ansatz in der heutigen Zeit noch gültig ist, oder ob sich das Daten-

schutzgesetz wandeln muss. Es gibt fünf verschiedene Ansätze (Prof. Dr. Jarchow und Estermann, 2015, S. 19-20):

1. **Traditionell**: Personendaten (siehe Kapitel Datenschutz) sind besonders schützenswert, laut der aktuellen Rechtslage. Daten wie Name, Wohnort, Alter usw. sind öffentlich zugänglich.
2. **Big-Data-orientiert**: Besonders schützenswert sind Daten, die es ermöglichen, eine Person durch Kombination der Daten, zu identifizieren.
3. **Relativistisch**: Die Studie zeigt, dass die Auffassung, welche Daten schützenswert sind, je nach Kultur und Individuell oder je nach Verwendungszweck variiert. Es soll deshalb grundsätzlich keine Unterscheidung zwischen besonders und weniger schützenswerten Daten gemacht werden.
4. **Persönliche Datenhoheit**: „It's not about privacy, it's about control" – jede Person soll die Kontrolle über seine oder ihre Daten haben. Voraussetzung dafür wären fähige User sowie die entsprechende technische Infrastruktur.
5. **Unversehrte digitale Identität**: Gemäss diesem Ansatz soll die digitale in gleichem Masse wie die physische Identität geschützt werden. Insbesondere sollen die Daten richtig sein, damit Falschinformationen nicht zu Diskriminierungen führen können.

2015 gab die PostFinance bekannt, dass sie die E-Banking-Daten Ihrer Kundinnen und Kunden auswerten wolle. Dies hat eine Welle der Entrüstung ausgelöst. Wer sich einloggte erhielt neue AGB, denen er zustimmen musste, um das E-Banking weiter nutzen zu können. Einerseits stiess dieses Vorgehen, andererseits die geplante Nutzung der Kontodaten durch Dritte bei vielen auf Unverständnis. Der Datenschutzbeauftragte griff ein. Die Kundschaft der PostFinance müsse transparent informiert werden sowie freiwillig zustimmen. Die PostFinance hat eingelenkt. Die User können nun ausschliessen, dass ihre Daten für diese Zwecke verwendet werden können. Viele User hätten aber bereits den neuen AGB zugestimmt, wohl ohne sich der Konsequenzen bewusst zu sein. Dies deutet auf eine ungenügende Sensibilisierung der Gesellschaft hin. Der Konsumentenschutz zeigt sich erfreut über diese Änderung, wie gross der Imageschaden für die PostFinance ist, kann nicht eingeschätzt werden (Kohler, 2015).

**Datenmonopole** (Risiko 11)

Die Welt teilt sich in zwei Teile: wenige Daten-Monopole stehen der Masse an Personen gegenüber, die über keine Daten verfügen. Dies führt zu sozialer und wirtschaftlicher Ungleichheit (Prof. Dr. Jarchow und Estermann, 2016, S. 22).

Big Data kann von hohem Nutzen sein für die Gesellschaft sowie für die Wirtschaft, schreibt Guy Verhofstadt, Autor der Frankfurter Allgemeinen (2014). Doch in den Händen von den sogenannten „Big Companies / Governments" könne dieses Wissen durchaus schädlich sein. Das Problem, das er hervorhebt ist jenes, dass ein einzelner Mensch in Daten zu ertrinken droht, da

man als Individuum keine Mittel hat, die Datenmenge auszuwerten. Grosse Unternehmen oder Staaten haben Kapital und somit die Möglichkeit. Verhofstadt plädiert dazu, dass alle Daten öffentlich gemacht werden – er nennt dies „Open-Source-Gesellschaft“. Dass also die Bürger Einblick erhalten in alle Daten, die vom Staat erhoben werden. So würden die Bürger als Individuen die Kontrolle über ihre Daten und somit über ihre Privatsphäre zurückerlangen, ganz nach dem Motto „Wissen ist Macht“. Wiederum würde die Transparenz des Staatsapparats und somit dessen Transparenz erhöht werden. Als zweiter Schritt müssten dann auch private Unternehmen transparenter mit ihren gesammelten Daten umgehen (ebd., 2014).

**Prognosen** (Chance 3, 4 und 5 sowie Risiko 13)
Als Tom Cruise 2002 im Hollywood-Blockbuster „Minority Report“ Kriminelle verhaftete, bevor diese die Tat begangen hatten, redete man von Science-Fiction. Doch seit dem Sommer 2014 testet die Stadtpolizei Zürich eine neue Software, mit der Verbrechen (primär Einbrüche) vorhergesehen werden können. Diese Software basiert auf einem Algorithmus, der Einbruchsdaten auswertet und ein Lagebild über mögliche zukünftige Einbrüche zu Verfügung stellt – in Echtzeit. Auch in der USA sind seit längerem solche Systeme im Einsatz. Dort gab es jedoch schon einige Male falsche Prognosen, die Konsequenzen für die betroffenen Personen hatten. Hanni Fakhoury der Electronic Data Foundation sagte:

> *„Eines der Probleme von Predictive Policing ist, dass letztlich jeder Algorithmus, der auf menschlichen Daten basiert, in das System eingespeist wird. Wenn Polizeiarbeit auf stereotypen oder gar rassistischen Profilen gründet, wird der Algorithmus einfach dieselben Ergebnisse ausspucken“ (Lobe, 2014).*

Fakhoury hält die Softwares noch für zu unreif für den Einsatz und warnt davor, Entscheidungen aufgrund dieser Algorithmen zu treffen. Zusätzlich kommt dazu, dass nur aufgrund früherer Muster Prognosen gemacht werden können. Folgt ein Verbrechen also keinem bekannten Muster, kann es auch nicht vorhergesagt werden. „Kriminalität ist kein blosses Rechenspiel, sondern ein komplexes Konstrukt aus Intention, Motivation und äusseren Umständen“ (Lobe, 2014).

Dies gilt nicht nur für Kriminalität. Auch beispielsweise Wettervorhersagen werden mit Hilfe von Big Data immer genauer. Das hilft zum Beispiel Werbern. Denn wenn sie wissen, dass die Pollensaison früh einsetzt, kann früher für Anti-Heuschnupfen-Mittel Werbung geschalten werden. Aber auch Versicherer können ihre Prämien anpassen, wenn sie genau wissen, in welchen Regionen Hagelstürme äusserst wahrscheinlich sind. Ermöglicht wird dies durch massenhaft Satelliten und Messstationen. Die Unmengen an Daten lassen die benötigte Rechenleistung explodieren. Der Deutsche Wetterdienst arbeitet mit 30'000 PCs. Besonders wichtig sind die genauen Wetterdaten auch für die Netzbetreiber (Scheppach, 2015).

> *„Wind und Wetter sind schwer kalkulierbar. Und je höher der Anteil fluktuierender erneuerbarer Energien wird, desto gefährdeter ist die Stabilität des Stromnetzes. Blackouts drohen. Auch hier können ausgeklügelte mathematische Rechenoperationen helfen“ (Scheppach, 2015).*

Es ist jedoch anzumerken, dass es auch gefährlich sein kann, sich bei Entscheiden immer auf Daten zu verlassen. Diese basieren nämlich immer auf der Vergangenheit (Dr. Prof. Jarchow und Estermann, 2016, S. 16).

# 4. Fazit

**Digitalisierung.** Dass die Welt immer mehr digital wird, kann nicht mehr ignoriert werden. In der Schweiz sind 100% der Jungen ständig am Netz und hinterlassen Datenspuren (Kapitel 1.1). Die Unternehmen oder auch Staaten, können sich diese Daten zu Nutzen machen. Die rohen Daten nützen jedoch nichts, sie müssen ausgewertet werden. Hier stellt sich die Herausforderung der 5 Vs: Das Volumen, die schnelle Vermehrung (Velocity), die Variation der Daten, die Relevanz (Veracity) und der Wert (Value) (Kapitel 2.1). Ausserdem beginnt der Datenschutz zu greifen, sobald ein Unternehmen oder ein Staat beginnt Daten zu bearbeiten – und die Bearbeitung beginnt schon beim Sammeln.

**Datenschutz.** Das Datenschutzgesetz (DSG) schützt die Persönlichkeit der Person, deren Daten bearbeitet werden. Das Recht auf Schutz vor Missbrauch der persönlichen Daten ist in der Schweiz sogar in der Verfassung verankert. Unternehmen, die Daten auswerten möchten, müssen sich an folgende Grundsätze halten: Rechmässigkeit, Verhältnismässigkeit, Zweckbindung, Erkennbarkeit und Einwilligung. Es gibt gewisse Ausnahmen, bei denen es keine Einwilligung braucht, beispielsweise bei einem Vertragsabschluss. Hier steht das Interesse der datenbearbeitenden Instanz über dem Interesse der Person. Wenn Daten bearbeitet werden, muss deren Schutz angemessen gewährleistet werden (Kapitel 2.2.1).

**Daten im Ausland.** Das DSG definiert auch Richtlinien für den Fall, dass Daten über die Landesgrenzen hinweg weitergegeben werden. Grundsätzlich muss das andere Land angemessenen Schutz bieten. Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) führt hierzu eine Liste. Die USA beispielsweise gilt als nicht sicheres Land, besonders nachdem das „Save Harbor“ Abkommen für ungültig erklärt wurde. Wenn der User seine Daten jedoch öffentlich zugänglich macht (z.B. über Google, Facebook, usw.), gilt der Schutz des DSG nicht mehr. Europa wird per 2018 ihre Datenschutzbestimmungen verschärfen (EU-Datenschutz-Grundverordnung) und die Schweiz wird nachziehen müssen. Unter anderem wird das Recht auf Vergessen sowie „Privacy by Default/Design“ als Standard eingeführt werden und US-Unternehmen werden an das EU-Recht gebunden. Ausserdem können hohe Bussgelder verlangt werden. Die Lösung für dem Umgang mit Big Data sollen pseudonymisierte Daten sein (Kapitel 2.2.2).

**AGB.** Gerade bei Online-Diensten sind AGB ein gängiges Mittel, um die Einwilligung der User einzuholen. Wichtig ist jedoch, dass der User eindeutig zustimmen muss. Auch müssen sie verständlich sein und Änderungen sowie ungewöhnliche Verwendungszwecke müssen klar kommuniziert und hervorgehoben werden (Kapitel 2.2.3).

**Anonymisierung.** Anonymisierte Daten werden grundsätzlich nicht durch das DSG geschützt. Können verschiedene anonymisierte Datenstränge durch zusammenführen jedoch zu einem Persönlichkeitsprofil führen, gelten sie wieder als schützenswert. Auch kann heute nicht garantiert werden, dass anonymisierte Daten mit der Technik von Morgen nicht entschlüsselt werden können (Kapitel 2.2.4).

**Chancen und Risiken.** Es konnten folgende fünf Chancen- und Risiko-Felder beim Thema Big Data identifiziert werden. Die Übergänge von Risiken zu Chancen und umgekehrt sind fliessend (Kapitel 3).

Marketing und Werbung:

- Personalisierte Werbung mit wenig Streuverlust ist attraktiv. Die Zielgruppe kann mittels Daten identifizert und gezielt angesprochen werden. Dazu brauchen die Unternehmen das Einverständnis der User (Opt-in).
- Für den User birgt extrem personalisiertes Marketing einige Risiken, wie beispielsweise das der „Filter Bubbles“.

Technologie:

- Um Big Data auswerten zu können, sind gute technische Lösungen notwendig. Für KMUs müssen standardisierte Systeme her, die u.a. mit ihrer bestehenden Datenbank kommunizieren können. Solche Standardsysteme sind noch nicht Realität.
- All diese Daten werden irgendwo gespeichert und sind somit dem Risiko von Cyber-Attacken ausgesetzt. In der Schweiz nimmt diese Art von Kriminalität stetig zu und viele Firmen geben zu, nicht darauf vorbereitet zu sein.
- Intelligente Systeme, sogenannte künstliche Intelligenz (KI), sollen helfen, die enormen Datenmengen mittels Algorithmen auszuwerten. Diese KIs können selbst lernen und die Daten selbstständig vernetzen. Der Suchmaschinenanbieter Google ist momentan der Vorreiter in der Entwicklung einer KI.
- Ein weiteres technologisches Feld ist das Internet of Things (IoT). Maschinen und Alltagsgegenstände sind miteinander verknüpft und produzieren Daten.

Datenschutz:

- Es gibt verschiedene Ansätze, wie das Spannungsfeld Datenschutz vs. Big Data gelöst werden könnte. Der traditionelle Ansatz, der Big-Data orientierte, der relativistische, der An-

satz der persönlichen Datenhoheit und derjenige der unversehrten digitalen Identität. Es wird sich zeigen, welcher sich durchsetzen wird.

- Das Reputationsrisiko ist gross, wenn gegen den Datenschutz verstossen wird. Dies musste beispielsweise die PostFinance 2015 feststellen, als sie die Daten der E-Banking-User auswerten wollte.

Datenmonopole:

- Die Welt ist zweigeteilt. Eine kleine Menge hält alle Daten, während die grosse Masse der Menschen keinen Zugriff auf ihre eignen Daten hat.
- Ein einzelner Mensch kann die Datenmenge nicht kontrollieren, da er oder sie gar nicht die Mittel dazu hat. Die sogenannten „Big Companies / Governments" haben diese Mittel jedoch. Viele plädieren für eine „Open-Source-Gesellschaft", bei der vom Staat aus maximale Transparenz geschaffen wird, um dem Bürger die Kontrolle über seine Daten zurückzugeben.

Prognosen:

- Dank den vielen verfügbaren Daten können vermehrt Prognosen in allen möglichen Bereichen gemacht werden. Beispielsweise bei der Polizeiarbeit oder beim Wetter.
- Das Riskiko bei solchen datenbasierten Prognosen ist jedoch, dass diese stets vergangenheitsorientiert sind. Ausserdem können sie zu falschen Schlüssen führen, wenn nicht auch etwas „gesunder Menschenverstand" benutzt wird.

**Schlussbemerkung**. Das Thema Big Data scheint vom „Gipfel der überzogenen Erwartungen" ins „Tal der Enttäuschung" gerutscht zu sein (Gartner, 2015). Es sind noch keine Wege gefunden worden, die Auswertung und Nutzung dieses Daten-Rohmaterials gewinnbringend und massentauglich (auch für kleinere Unternehmen) umzusetzen. Doch wie der Gartner-Hype-Zyklus sagt, wird dieses Thema bestimmt den „Pfad der Erleuchtung" finden und somit das „Plateau der Produktivität" erreichen. Zum heutigen Zeitpunkt ist die Technik sowie die Gesetzeslage noch nicht so weit. Doch Fortschritte wie sie Google mit der künstlichen Intelligenz macht, oder die Swisscom, die in der Schweiz ein eigenes Netz für das Internet of Things aufbaut, sind nur einige der Indikatoren, die zeigen, dass Big Data ein Thema der Zukunft bleibt. Die Unternehmen sowie der Staat und die Gesellschaft sind verpflichtet, sich den Risiken dieses Themas anzunehmen, denn die Thematik betrifft alle.

# 5. Reflexion

Diese Arbeit entstand im Rahmen des CAS Digital Risk Management (DRM) an der Hochschule für Wirtschaft in Zürich und beschäftigte sich mit dem Thema Chancen und Risiken von Big Data. Zuerst wurde der Begriff Big Data definiert. Dort stellte sich heraus, dass gerade der Datenschutz ein grosses Risiko darstellt. Deshalb wurde der Schweizerische Datenschutz genauer analysiert. Da viele Online-Dienste Daten ins Ausland übertragen, wurde auch die Gesetzeslage im Ausland betrachtet. Zum Schluss wurden konkrete Anwendungsfelder von Big Data und deren Chancen und Risiken näher ausgeführt. Alles entstand mit Hilfe von Literaturrecherche. Besonders die Studie, welche die Berner Fachhochschule durchführte, war sehr hilfreich. Diese lieferte repräsentative Umfrageergebnisse zu diesem Thema.

Das Feld Big Data ist sehr gross. Erkenntnisse aus Kundendaten könnten in so ziemlich allen Geschäftsfeldern und Branchen gewinnbringend verwendet werden. Doch besonders die Unsicherheiten bezüglich Datenschutz verhindern hier weiteres Vorankommen. Auch ist die Technik noch nicht soweit – oder zumindest noch nicht erschwinglich. Dies ist aus der Arbeit ersichtlich geworden.

Gerade die Grösse des Themenfelds bereitete mir gewisse Schwierigkeiten. Es war nicht einfach, einen roten Faden hineinzubringen. Und gerade beim Kapitel 3 „Chancen und Risiken“ hätte ich noch zehn weitere Seiten mit Anwendungsbeispielen und entsprechenden Risiken schreiben können. Auch ist dieses Feld noch sehr wenig erforscht. Vielfach stiess ich auf Anwendungsberichte von spezifischen Unternehmen oder Branchen. Allgemeine Informationen sind selten.

Für kleinere Unternehmen sehe ich enormes Potential. Denn gerade bei kleinem Budget sollte beispielsweise die Zielgruppe möglichst genau angesprochen werden. Hier fehlen noch standardisierte und erschwingliche Lösungen. Auch bei Prognosen sehe ich grosses Potential, auch wenn hier der gesunde Menschenverstand nie ausser Acht gelassen werden darf. Beispielsweise bei der Stromversorgung kann mit Hilfe von Datenanalysen die sinnvolle Verteilung resp. die Aufrechterhaltung besser gewährleistet werden.

Die Welt hat noch viel zu lernen im Bereich Big Data. Was sie bestimmt auch tun wird in den nächsten Jahren. Datenanalysen bergen viele Gefahren und Risiken, aber wie so oft, ist genau dort das Potential enorm gross.

# III. Quellenverzeichnis

Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS. (2010). Schweizerische Eidgenossenschaft, Bern.

BR News. (2016). EU-Datenschutzgrundverordnung (DSGVO): Alles Neue zur Datenschutzreform. Abgerufen 15. Mai, von http://br-news.ch/dsgvo-eu-datenschutzgrundverordnung-alles-neue-zur-datenschutzreform/

Bundesamt für Statistik. (2016a). Haushalte und Bevölkerung - Internetnutzung. Abgerufen am 21. März 2016, von http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html

Bundesamt für Polizei fedpol. (2015). Jahresbericht 2014. Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK. Schweizerische Eidgenossenschaft, Bern.

Bundesgesetz gegen den unlauteren Wettbewerb. (Stand 2014). Schweizerische Eidgenossenschaft, Bern.

Bundesgesetz über den Datenschutz (DSG). (Stand 2014). Schweizerische Eidgenossenschaft, Bern.

Bundesverfassung der Schweizerischen Eidgenossenschaft. (Stand 2016). Schweizerische Eidgenossenschaft, Bern.

Cheesman Patrick. (2016). How Big Data Can Transform Your Understanding Of Your Customers. Aberufen 4. April 2016, von http://www.patrickcheesman.com/how-big-data-can-transform-your-understanding-of-your-customers/

Datenschutzbeauftragter. (2015). EU-Datenschutz-Grundverordnung: Das sind die Neuerungen. Abgerufen 5. Mai 2016, von https://www.datenschutzbeauftragter-info.de/eu-datenschutzgrundverordnung-das-sind-die-neuerungen/

Dr. Eckert Martin. (2016). Unterrichtsfolien CAS Digital Risk Management: New Technologies - Big Data. Zürich.

Dr. Widmer & Partner - Rechtsanwälte. (2015). EU-Datenschutzgrundverordnung wird Realität - Was gilt für Sie? Abgerufen 15. Mai, von http://www.widmerpartners-

lawyers.ch/index.php?id=63&L=1'%22&tx_ttnews%5Btt_news%5D=1047&cHash=129f2921cdcec0df4618dba7151f189d

Drösser Christoph. (2015). Maschinen sind die Denker von morgen. Zeit online, 24. April 2014, von http://www.zeit.de/kultur/film/2015-04/kuenstliche-intelligenz-ex-machina-big-data/komplettansicht

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2008/2009). Abschluss eines Safe-Harbor-Abkommens Schweiz-USA. Schweizerische Eidgenossenschaft, Bern.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2015a). Safe-Harbor-Urteil des Europäischen Gerichtshofs: Stellungsnahme des EDÖB. Schweizerische Eidgenossenschaft, Bern.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2015b). Nach Safe-Harbor-Urteil: Hinweise zur Datenübermittlung in die USA. Schweizerische Eidgenossenschaft, Bern.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2016a). Erläuterungen zu Big Data. Abgerufen 4. April 2016, von http://www.edoeb.admin.ch/datenschutz/00683/01169/01344/index.html

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (2016b). Stand des Datenschutzes weltweit. Schweizerische Eidgenossenschaft, Bern.

eMarketer. (2014, Dezember 11). 2 Billion cnsumers worldwide to get smart(phones) by 2016.

Gartner. (2015). Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. Abgerufen 11. Juni 2016, von http://www.gartner.com/newsroom/id/3114217

Internet live stats. (2016). 1 second. Abgerufen 21. März 2016, von http://www.internetlivestats.com/one-second/

Kasack Hendrick. (2016). Neue EU-Datenschutzregeln. Im Tausch gegen Daten. Frankfurter Allgemeine Wirtschaft, 18. Dezember 2015, von http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/was-taugt-die-eu-datenschutz-verordnung-13972055.html

Kohler Franziska. (2015). Postfinance muss E-Banking Portal ändern. Tages Anzeiger, 3. Juni 2015. Abgerufen am 5. Juni 2016, von http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Postfinance-muss-EBankingPortal-aendern/story/17331328

Lobe Adrian. (2014). "Minority Report" in Zürich. Tages Anzeiger, 5. Dezember 2014. Abgerufen am 22. Mai 2016, von http://www.tagesanzeiger.ch/zuerich/stadt/Minority-Report-in-Zuerich/story/12692897

Loy Elisa. (2016). Security-Studie von VMware. „Eine generelle IT-Sicherheitslösung wird es nicht geben". CRN.de, 03. Juni 2016, abgerufen 11. Juni 2016, von http://www.crn.de/security/artikel-110445.html

Naisbitt John. (1984). Megatrends. Ten New Directions Transforming Our Lives. Warner Books.

OECD. (2015). Digital Economy Outlook 2015. Paris, Frankreich: OECD Publishing.

PC-Magazin. (2014). Chancen und Risiken von Big Data. Aufgerufen 22. Mai 2016, von http://www.pc-magazin.de/business-it/chancen-und-risiken-von-big-data-2143274.html

Prof. Dr. Jarchow Thomas und Estermann Beat. (2015). Big Data: Chancen, Risiken und Handlungsbedarf des Bundes. Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation. Berner Fachhochschule, E-Government-Institut. Bern.

Sander Matthias. (2015). Hinter dem Hype um das "Internet der Dinge". Neue Zürcher Zeitung, 26. März 2015, von http://www.nzz.ch/wirtschaft/was-hinter-dem-hype-um-das-internet-der-dinge-steckt-1.18510918

Scheppach Joseph. (2015). Und jetzt: Ihr Wetter. Technology Review, 6. Mai 2015. Abgerufen am 22. Mai 2016, von http://www.heise.de/tr/artikel/Und-jetzt-Ihr-Wetter-2599595.html

Schwägerl Christian. (2016). Vorsicht vor der digitalen Weltpolizei. Frankfurter Allgemeine Feuilleton, 31. März 2016, von http://www.faz.net/aktuell/feuilleton/debatten/warum-die-kuenstliche-intelligenz-gefahren-birgt-14151739.html?printPagedArticle=true#pageIndex_2

Springer Gabler Verlag (Hrsg.). (2016a). Gabler Wirtschaftslexikon, Stichwort: Big Data. Aberufen 31.März 2016, von http://wirtschaftslexikon.gabler.de/Archiv/-2046774198/big-data-v3.html

Springer Gabler Verlag (Hrsg.). (2016a). Gabler Wirtschaftslexikon, Stichwort: Data Mining. Aberufen 31.März 2016, von http://wirtschaftslexikon.gabler.de/Archiv/57691/data-mining-v8.html

Sweeney Latanya. (2000). Simple Demographics Often Identify People Uniquely. Abstract. Abgerufen 20. Mai 2016, von http://repository.cmu.edu/isr/230/

Swisscom. (2016). Swisscom baut en schweizweites Netz für das Internet der Dinge. Abgerufen 5. Juni 2016, von https://www.swisscom.ch/de/about/medien/press-releases/2016/03/20160314-MM-Internet-der-Dinge.html?utm_content=bufferece0e&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Thiel Thomas. (2012). Eli Pariser: "Filter Bubble". Im Netz wartet schon der übermächtige Doppelgänger. Frankfurter Allgemeine Feuilleton, 07. März 2012, von http://www.faz.net/aktuell/feuilleton/buecher/rezensionen/sachbuch/eli-pariser-filter-bubble-im-netz-wartet-schon-der-uebermaechtige-doppelgaenger-11675351.html?printPagedArticle=true#pageIndex_2

Vasella, D. (2015). Kapitel 7: Social Media und Datenschutz. In Staffelback O. und Keller C. (Hrsg). Social Media und Recht für Unternehmen (S. 241-308). Zürich, Basel, Genf: Schulthess Juristische Medien AG.

Verhofstadt Guy. (2014). Plädoyer für eine Open-Source-Gesellschaft. Wir müssen Big Data beherrschen! Frankfurter Allgemeine Feuilleton, 2. Mai 2014. Abgerufen 22. Mai 2016, von http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/plaedoyer-fuer-eine-open-source-gesellschaft-wir-muessen-big-data-beherrschen-12920338.html?printPagedArticle=true#pageIndex_2

Zeier Rafael. (2016). Fünf Tricks gegen die Filterblase. Tagesanzeiger, 10. Februar 2016, von http://www.tagesanzeiger.ch/digital/social-media/fuenf-tricks-gegen-die-filterblase/story/25311463