

# Big Data: Chancen, Risiken und Handlungsbedarf des Bundes

Ergebnisse einer Studie im Auftrag des  
Bundesamts für Kommunikation

Prof. Dr. Thomas Jarchow  
Beat Estermann

Version 1.0  
26. Oktober 2015

Berner Fachhochschule  
E-Government-Institut

Dieses Dokument untersteht der Creative Commons Namensnennung 4.0 Lizenz  
(CC BY 4.0).

**Titelbild:** Wassily Kandinsky (1866-1944), Komposition 8 (1923), Guggenheim Museum,  
New York, Public Domain.

## Das Wichtigste in Kürze

Der Begriff „Big Data“ bezeichnet die Entwicklung und den Einsatz von Technologien, welche es erlauben, dem richtigen Nutzer zur rechten Zeit die richtigen Informationen aus den in unserer Gesellschaft seit längerem exponentiell anwachsenden Datenbeständen zu liefern. Dabei besteht neben der Herausforderung, immer grössere Datenvolumen in immer kürzerer Zeit zu verarbeiten, auch die Schwierigkeit, mit der zunehmenden Heterogenität der Formate, der Komplexität und der Verlinkung der Daten fertig zu werden.

Angesichts der rasanten Ausbreitung von Big Data setzt sich der Bund im laufenden Jahr mit dieser Thematik auseinander. Vor diesem Hintergrund führte die Berner Fachhochschule im Auftrag des Bundesamts für Kommunikation die vorliegende Studie durch. Sie besteht aus einer qualitativen Befragung von 20 Experten aus Wirtschaft, Verwaltung und Zivilgesellschaft und einer quantitativen Erhebung bei über 800 Personen in der Schweiz. Ziel der Studie ist es, die Chancen und Risiken von Big Data zu identifizieren und den Handlungsbedarf des Bundes aufzuzeigen.

Beim Phänomen „Big Data“ handelt es sich um eine allmähliche Entwicklung infolge grösserer Analyse- und Speicherkapazitäten, die sich dadurch manifestiert, dass immer grössere Mengen von teils heterogenen Daten verarbeitet und miteinander verknüpft werden. Damit handelt es sich bei Big Data um eine Entwicklung, die nach und nach immer weitere Bereiche der Wirtschaft und Gesellschaft erreicht.

Big Data bringt bedeutende Chancen und Vorteile mit sich, wie zum Beispiel das Gewinnen neuer Erkenntnisse und Entdecken neuer Zusammenhänge, die Personalisierung von Angeboten und Informationen, verbesserte Prognosen in ganz unterschiedlichen Bereichen, eine erhöhte Agilität von Unternehmen und Organisationen, die Optimierung von Abläufen sowie die Möglichkeit, Entscheide vermehrt faktenbasiert zu fällen.

Allerdings setzt die erfolgreiche Anwendung von Big Data in Unternehmen organisatorische Anpassungen und einen kulturellen Wandel voraus. Die Experten-Interviews haben gezeigt, dass sich einige Unternehmen und Organisationen bereits an die neuen Gegebenheiten angepasst haben, indem sie die notwendigen Vorkehrungen getroffen haben, um Chancen von Big Data wahrnehmen und Risiken besser unter Kontrolle halten zu können, während sich andere erst anschicken, auf den Big-Data-Zug aufzuspringen.

Die Studie zeigt aber auch, dass die gesellschaftlichen Implikationen von Big Data stärker in den Fokus genommen werden sollten. Die drängendsten Fragen stellen sich im Bereich des Schutzes von Personendaten bzw. bei der Prävention von Daten-Missbrauch. Einzelne Stimmen warnen zudem vor der unkontrollierten Eigendynamik der Systeme, wenn immer mehr Entscheide auf Algorithmen basieren, die niemand mehr richtig versteht und beherrscht. Ein weiterer Problemkreis, für den Big Data nicht ursächlich ist, auf den sich Big Data aber verschärfend auswirken dürfte, ist die ungleiche Verteilung von Ressourcen und Macht, welche die Gefahr von gesellschaftlichen Verwerfungen birgt, falls nicht rechtzeitig Gegensteuer gegeben wird.

Neben der Abwehr von Gefahren sollte auch die Förderung des Potentials von Big Data nicht zu kurz kommen. Hier herrscht weitgehend Einigkeit darüber, dass der gesellschaftliche Nutzen von Daten sich erhöht, wenn sie als freie Infrastruktur-Ressourcen verfügbar sind und von den verschiedenen Akteuren möglichst unkompliziert weiterverwendet werden können. Dies gilt in erster Linie für nicht-personenbezogene Daten; bei den personenbezogenen Daten ist die Situation komplizierter, da es zunächst neuer Mechanismen bedarf, die es den Einzelnen erlauben, die Kontrolle über ihre Daten effektiv wahrzunehmen und die Daten gezielt – und nicht völlig unkontrolliert, wie dies heute oftmals geschieht – für bestimmte Zwecke zur Weiterverwendung zur Verfügung zu stellen.

Wie aus den Umfrageergebnissen hervorgeht, stellt sich die grundsätzliche Herausforderung, die Entwicklungen im Bereich Big Data so zu kanalisieren, dass sie zum Nutzen der Menschen reichen. Heute scheinen vor allem grössere Unternehmen von Big Data zu profitieren, während die Befragten die Situation aus ihrer persönlichen Sicht eher kritisch beurteilen und ein starkes Engagement des Bundes fordern, um die Situation nicht aus dem Ruder laufen zu lassen. Dabei erscheint eine Drei-Punkte-Strategie angezeigt:

**Aufbau und Pflege einer nationalen Dateninfrastruktur:** Die positive Wirkung von Big Data kann durch die Bereitstellung von Daten als Infrastrukturressource zur freien Weiterverwendung verstärkt werden. Es gilt daher, dem im Rahmen der bundesrätlichen Open-Government-Data-Strategie etablierten Open-Data-Prinzip über die gesamte Verwaltung hinweg, in der Forschung und teilweise auch in der Privatwirtschaft zum Durchbruch zu verhelfen und es konsequent umzusetzen. Zudem sollte in enger Zusammenarbeit mit der Privatwirtschaft die Standardisierung von technischen Schnittstellen vorangetrieben und die Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists u.ä.) gefördert werden. Ziel sollte es sein, eine national koordinierte und international vernetzte Dateninfrastruktur zu schaffen.

**Massnahmen zum Schutz vor Missbräuchen:** Um Missbräuchen und Ungleichgewichten entgegenzuwirken, sollten die Datenschutzregeln für die Privatwirtschaft verschärft, die wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internetbereich verstärkt und Aufklärungs- und Sensibilisierungsmassnahmen durchgeführt werden. Zudem müssen die rechtlichen Rahmenbedingungen für sichere Datenzentren verbessert werden. In enger Kooperation mit der Privatwirtschaft sollten zudem vermehrt technische Lösungen entwickelt werden, um den Datenschutz sicherzustellen. Viele dieser Massnahmen weisen allerdings die Schwierigkeit auf, dass sie international koordiniert werden müssen, um wirksam zu sein.

**Umsetzung des Prinzips der persönlichen Datenhoheit:** Als langfristige Lösung sollte beim Datenschutz ein Paradigmenwechsel eingeleitet werden, indem die Menschen befähigt werden, die Kontrolle über ihre Daten besser auszuüben. Zur Umsetzung des Prinzips der persönlichen Datenhoheit müssen im Bereich der personenbezogenen Daten neue Eigentums- und Nutzungsrechte definiert werden. Zudem gilt es, in enger Kooperation mit der Privatwirtschaft Mechanismen zu schaffen und Dienste bereitzustellen, welche es den Einzelnen erlauben, ihre personenbezogenen Daten – unter grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben. Auch hier sind die Anstrengungen international zu koordinieren. Während die Realisierung dieses liberalen Ansatzes zur Behebung der Ungleichgewichte auf dem Datenmarkt heute noch in weiter Ferne liegen mag, geniesst er als Zielvorgabe bei allen Anspruchsgruppen breite Unterstützung.

Auf der Basis der Studienergebnisse wurden mit Blick auf eine „Good Data Governance“ sieben Thesen formuliert, die bei der Umsetzung einer Big-Data-Strategie als Orientierungshilfe dienen können:

1. Beim Datenschutz braucht es einen Paradigmenwechsel in Richtung Empowerment der Nutzer und persönlicher Datenhoheit.
2. Der gesellschaftliche Nutzen von Daten erhöht sich, wenn sie als freie Infrastruktur-Ressourcen verfügbar sind.
3. Big Data verschärft eine Reihe von Gefahren, die abgewehrt werden müssen; hinsichtlich der Bedrohung der Privatsphäre und der missbräuchlichen Verwendung von Daten erhöht Big Data nicht nur die Eintrittswahrscheinlichkeit eines Schadens, sondern auch dessen potentielles Ausmass.
4. Gegen Machtgefälle aufgrund von einseitiger Datenkontrolle müssen Massnahmen ergriffen werden; insbesondere die (Quasi-)Monopolisten im Internet-Bereich müssen in die Schranken gewiesen werden.
5. Es sollte ein liberaler Ansatz verfolgt werden: Ziel ist ein System, bei dem der Markt dank eines Empowerment der Nutzerinnen und Nutzer und einer stärkeren Regulierung und Kontrolle der privatwirtschaftlichen Akteure durch den Staat besser funktioniert als heute.
6. Staatliche Intervention ist nötig: Ohne ein starkes Engagement des Staates wird die Entwicklung im Zusammenhang mit Big Data aus dem Ruder laufen, denn es steht ausser Zweifel, dass der Markt heute im Bereich der Daten versagt.
7. Data Governance muss im internationalen Kontext angegangen werden. Es liegt daher nahe, sich bei der konkreten Ausgestaltung der zu treffenden Massnahmen von Lösungsansätzen inspirieren zu lassen, die bereits in anderen Ländern erprobt werden.

# Inhaltsverzeichnis

Das Wichtigste in Kürze	3
1 Einleitung	6
2 Methodologisches Vorgehen	11
3 Bedeutung von Big Data für Wirtschaft und Gesellschaft	14
4 Grundlagen der Data Governance auf gesellschaftlicher Ebene	19
5 Sieben Thesen hinsichtlich einer „Good Data Governance“	27
6 Ergebnisse der quantitativen Erhebung	29
7 Implikationen für eine „Good Data Governance“	76
8 Fazit und Ausblick	84
9 Literaturverzeichnis	86
Anhang 1: Interview-Leitfaden für „Akteure mit Big Data“	88
Anhang 2: Interview-Leitfaden für „Beobachter von Big Data“	90
Anhang 3: Fragebogen	91
Anhang 4: Rücklaufquoten der verschiedenen Kategorien von Umfrageteilnehmern	108
Anhang 5: Liste sämtlicher Massnahmen	109
Anhang 6: Analyse der Abschnitte B und C des Fragebogens	116

# 1 Einleitung

Die zunehmende Verwendung von Daten in immer mehr Bereichen von Wirtschaft und Gesellschaft bietet neue Chancen, stellt uns aber auch vor neue Herausforderungen. Dabei wird der aktuelle Trend hin zur Analyse von immer grösseren Datenmengen, zum Zusammenführen von Daten aus ganz unterschiedlichen Quellen und zur immer schnelleren Verarbeitung von Daten gemeinhin unter dem Oberbegriff „Big Data“ zusammengefasst. Mit dem „Big Data“-Begriff verbunden werden bisweilen auch neue Analyse-Methoden, wie die Mustererkennung, welche es erlauben, mittels der Analyse von Daten ohne vorangehende Hypothesenbildung Voraussagen oder Entscheidungen zu treffen.

Angesichts der rasanten Ausbreitung von Big Data setzt sich der Bund im laufenden Jahr mit dieser Thematik auseinander. Vor diesem Hintergrund führte die Berner Fachhochschule im Auftrag des Bundesamts für Kommunikation eine Studie zu Chancen und Risiken von Big Data für Wirtschaft und Gesellschaft in der Schweiz durch, welche insbesondere auch den Handlungsbedarf des Bundes in diesem Bereich aufzeigt. Die Studie besteht aus einem Einführungsteil und zwei empirischen Teilen – einer Expertenbefragung und einer quantitativen Erhebung:

Kapitel 1 enthält eine kurze Einführung in die „Big Data“-Thematik, während Kapitel 2 das im Rahmen der Studie angewandte methodologische Vorgehen darlegt.

Kapitel 3 bis 5 enthalten die Ergebnisse der Expertenbefragung: In Kapitel 3 wird die Bedeutung von Big Data für Wirtschaft und Gesellschaft aufgezeigt, während in Kapitel 4 im Detail auf die Grundlagen der Data Governance eingegangen wird. Kapitel 5 enthält schliesslich die kondensierten Erkenntnisse aus der Expertenbefragung in Form von sieben Thesen hinsichtlich einer „Good Data Governance“.

Kapitel 6 und 7 enthalten die Ergebnisse der quantitativen Erhebung: In Kapitel 6 werden die Ergebnisse der Befragung im Detail vorgestellt und anschliessend in Kapitel 7 vor dem Hintergrund der sieben Thesen hinsichtlich einer „Good Data Governance“ diskutiert.

Den Abschluss bildet Kapitel 8 mit einem Fazit bezüglich der im Rahmen der Studie gewonnenen Erkenntnisse und einem Ausblick.

## 1.1 Big Data – Eine kurze Einführung

Während die weltweit verfügbare Datenmenge schon seit geraumer Zeit wächst, hat sich das Wachstum in den letzten Jahrzehnten dramatisch beschleunigt: Zur Zeit von Johannes Gutenberg verdoppelte sich die Menge verfügbarer Bücher noch etwa alle 50 Jahre (Eisenstein, 1993, S. 13ff). In den 20 Jahren zwischen 1987 und 2007 hat sich die Datenmenge in etwa ver Hundertfacht (Hilbert & López, 2011), was einer Verdoppelung circa alle drei Jahre gleichkommt. Um 2010 verdoppelte sie sich bereits etwa alle 2 Jahre (Gantz & Reinsel, 2011). Bereits Naisbitt (1982) hatte in den Achtziger Jahren des 20. Jahrhunderts festgestellt, dass wir „heute“ in Informationen ertrinken, es uns aber nach Wissen dürstet. Die allgegenwärtige und immer rascher fortschreitende Digitalisierung der gesamten Welt hat weitreichende Auswirkungen und einen beträchtlichen Einfluss auf Gesellschaft, Wirtschaft und Wissenschaft (Bryant, Katz, & Lazowska, 2008). Dabei sind auch traditionell nicht-technische Bereiche der Gesellschaft immer stärker betroffen, was nicht ohne Auswirkungen auf das politische Interessengefüge bleibt. So fühlen sich beispielsweise die in den digitalen Welten grossgewordenen „Digital Natives“ durch die traditionellen politischen Parteien bisweilen nicht mehr vertreten, was einige Kommentatoren zur Bemerkung verleitet hat, dass es neben den „rechten“, „konservativen“, „sozialen“, „grünen“ und „liberalen“ Parteien in Zukunft wohl auch noch eine „digitale“ Partei geben müsse (Keuper, Hamidian, Verwaayan, Kalinowski, & Kraijo, 2013, S. 5f).

Der Begriff „Big Data“ wurde zunächst für Problemstellungen bei der Visualisierung grosser Datenvolumen verwendet (Cox & Ellsworth, 1997). In der praktischen Anwendung zeigte sich, dass neben dem Datenvolumen („Volume“) auch die Dimensionen Geschwindigkeit („Velocity“) und Vielfalt („Variety“) (Laney, 2001) eine zentrale Rolle spielen. Darüber hinaus wird bisweilen auch auf die wichtige Rolle der Datenqualität („Veracity“) hingewiesen (vgl. Page et al., 2012; Schroeck, Shockley, Smart, Romero-Morales, & Tufano, 2012; Winter, 2011). Keine der dieser Dimensionen und auch keine Kombination davon sind grundsätzlich neu. Neu an Big Data ist, dass die Nutzung von Daten in allen Bereichen stark zunimmt, dass die Auswertung systematisch durchgeführt wird, und dass der

Datenzusammenzug massiv über bestehende Domänengrenzen hinausgeht, wie dies beispielsweise beim Zuwachs an verfügbaren Datenquellen im Internet of Things oder in der Kombination verschiedener personenbezogener Sensordaten im Social Mobile Computing zu beobachten ist. Mit zunehmendem Reifegrad der Technologie verschiebt sich der Fokus von Big Data von der Technologie und prototypischen Testanwendungen hin zu Fragen der Implementierung in der realen Welt, zur Anwendung von Big Data und zu deren Auswirkungen auf alle Bereiche der Gesellschaft und Wirtschaft. Daher sind in der wissenschaftlichen Auseinandersetzung mit dem Phänomen „Big Data“ in den letzten Jahren zu den drei bzw. vier klassischen V-Dimensionen weitere hinzukommen, wie „Business Value“, „Governance“ oder „People“ (Mysore, 2013). Heute stehen in der Big-Data-Debatte denn auch Fragestellungen rund um die organisatorische, gesellschaftliche, politische und juristische Einbettung der neuen Technologie im Vordergrund.

Zusammenfassend können wir unter Big Data die Entwicklung und den Einsatz von Technologien verstehen, welche es erlauben, dem richtigen Nutzer<sup>1</sup> zur rechten Zeit die richtigen Informationen aus den seit längerem exponentiell anwachsenden Datenbeständen zu liefern. Dabei besteht neben der Herausforderung, immer grössere Datenvolumen in immer kürzerer Zeit zu verarbeiten, auch die Schwierigkeit, mit der zunehmenden Heterogenität der Formate, der Komplexität und der Verlinkung der Daten fertig zu werden (Chen, Chiang, & Storey, 2012; Lycett, 2013).

Der folgende Abschnitt enthält einen kurzen Abriss der gesellschaftlich relevanten Aspekte von Big Data, die in der wissenschaftlichen Literatur diskutiert werden. Eine ausführlichere Abhandlung etlicher dieser Aspekte ist im kürzlich erschienen Bericht der OECD zu „Data Driven Innovation“ zu finden (OECD 2015).

## 1.2 Gesellschaftlich relevante Aspekte von Big Data

### 1.2.1 Daten und Datenzugang

Anbieter von Internetplattformen, Netzwerken und Social Media haben einen deutlichen Vorteil beim Zugang zu Daten und somit für datenbezogene Geschäftsmodelle. Dies führt zu einer ausgeprägten Asymmetrie im Markt, insbesondere da das Anlegen und die Pflege von Datensammlungen sowohl zeit- als auch ressourcenintensiv sind (Manyika et al., 2011, S. 107ff).

Für die gewöhnliche Nutzerin ist häufig nicht direkt ersichtlich, welche Daten zu welchem Zeitpunkt und in welchem Kontext über sie und ihr Verhalten gesammelt werden. Dies schränkt die Möglichkeiten ein, die gesammelten Daten zu prüfen und zu korrigieren (Redman, 2013).

Für Akteure, welche von Dritten generierte Daten weiterverwenden, besteht eine generelle Unsicherheit bezüglich Bedeutung, Genauigkeit und Aktualität der Daten, welche beispielsweise unvollständig, inkonsistent oder mehrdeutig sein können (Letouzé, 2012). Je spezifischer die Fragen sind, welche mit den Daten beantwortet werden sollen, desto wichtiger werden deren Qualität, Aktualität und der Kontext aus dem sie stammen (Walsh & Möhring, 2014).

Was die methodologischen Aspekte betrifft, stellt sich die Frage, inwieweit heutige statistische Verfahren für den Umgang mit Big Data überhaupt tauglich sind: Das wiederholte Auswerten der gleichen Datenbestände und das zunehmende Datenvolumen führen zu einer grösseren Anzahl zufällig signifikanter Treffer. Eine „neue“ Statistik, welche solche Probleme löst und zudem Unsicherheit, Bedeutung und Kontext der Daten berücksichtigt, ist noch nicht etabliert (McAfee & Brynjolfsson, 2012).

### 1.2.2 Ethischer Umgang und Reputation

Angesichts des zunehmenden Austauschs und der Verknüpfung von Daten aus unterschiedlichen Quellen besteht vor allem in grösseren Organisationen die Herausforderung, allgemeingültige Werte und Richtlinien über Kultur-, Sprach-, Interessens-, Hoheits-, und andere Grenzen hinweg einzuführen (Rivers & Lewis, 2014). Dies gilt auch für Richtlinien, welche sensible (z.B. private, vertrauliche) Daten betreffen, wie sie beispielsweise im Gesundheitsbereich heute üblich sind (Horvitz & Mulligan, 2015).

<sup>1</sup> Aus sprachökonomischen Gründen verzichten wir auf die systematische Nennung beider Geschlechter; das andere Geschlecht ist jeweils mitgemeint.

Bei der Auswertung von Daten besteht ein grundsätzlicher Interessenskonflikt zwischen einer breiten und vielfältigen Nutzung und einem engen Schutzbedürfnis. Dies betrifft die Bereiche Identität, Privatsphäre, Eigentumsrecht und Reputation (Berinato, 2014).

## 2 Der Umgang der Gesellschaft mit Big Data

Für Unternehmen und Organisationen existieren heute latente Risiken von unbeabsichtigten Folgen rechtlicher Art und auch bezüglich der Qualität ihrer Kundenbeziehungen, wenn sie mit den anvertrauten Daten unvorsichtig umgehen. Besonders kritisch sind falsche, nicht-anonymisierte oder re-identifizierbare Daten mit Personenbezug (El Emam, Jonker, Arbuckle, & Malin, 2011).

Datennutzung steht in einem facettenreichen Spannungsfeld von Sprache und Kultur, Art der Daten und bezweckter Nutzung, Trends und News, etc. Dabei haben die Faktoren (1) Vertrauen in die Organisation, (2) Preis-Leistungs-Verhältnis, (3) bisherige Erfahrungen und (4) Empfehlungen aus dem sozialen Umfeld (Familie, Freunde) den stärksten Einfluss darauf, ob ein Kunde seine persönlichen Daten preisgibt. Daher haben grosse und bekannte Organisationen einen impliziten Vorteil gegenüber kleinen oder unbekannteren Organisationen (ausschlaggebend sind insbesondere die Dimensionen Vertrauen, Bekanntheit und Stabilität) (vergl. Manovich, 2011). Über die ganze Gesellschaft hinweg gesehen, besteht eine bemerkenswerte und deutliche kognitive Dissonanz zwischen der Tatsache, dass „alle“ sich vor dem „gläsernen Bürger“ fürchten und der Tatsache, dass „alle“ einen Facebook-Account haben (Hsuan, 2011).

### 2.1 Big Data innerhalb der Organisation

Für Organisationen stellt Big Data auf verschiedenen Ebenen eine Herausforderung dar. Big Data geht häufig mit einem Umbau interner Strukturen für Datenhoheiten, Zugriffsrechte, etc. einher. Dabei stellt sich beispielsweise die Frage, ob Big Data in betriebswirtschaftlichen oder technologischen Abteilungen untergebracht wird. Die klare Verteilung von Rollen und Verantwortlichkeiten für Big Data ist erst im Entstehen begriffen und daher sind die internen Reibungsverluste noch hoch (mangelnde Akzeptanz, strategische Orientierung). Zudem laufen betriebliche Bonus-Anreizsysteme oftmals Regelungen bezüglich der Nutzung von sensiblen Informationen zuwider (Michael & Miller, 2013).

Die Nachfrage an Fachkräften ist derzeit hoch. Dabei sind die gesuchten Profile noch unscharf, was das Personalmanagement kostenintensiv und die Rekrutierung unsicher macht. Daher hängt der Erfolg von Big Data zurzeit stark vom verfügbaren Budget ab. Die Ausbildung von Fachkräften hat erst begonnen (Davenport & Patil, 2012), und Big-Data-Ökosysteme mit Strategien und Ausführungsplänen befinden sich erst im Aufbau.

### 2.2 Handlungsrichtlinien

Für Daten gibt es weniger rechtliche Handlungsrichtlinien als z.B. für den Umgang mit Vermögenswerten. Es sind aber intensive Bestrebungen im Gange, solche zu erstellen (siehe Europäische Kommission, 2014). Wie bei allen rechtlichen Anpassungen besteht das Risiko, dass Organisationen ihre Aktivitäten in weniger restriktive Rechtshoheiten verlagern (van Wel & Royakkers, 2004).

Aus Sicht multinationaler Big-Data-Bestrebungen wären länderübergreifende und konsistente Rechtslagen hilfreich. Diese setzen aber komplexe Verhandlungen voraus, die sehr kostenintensiv und äusserst langwierig sind. Eine internationale Harmonisierung ist daher in absehbarer Zeit eher unwahrscheinlich.

### 2.3 Technologie

Die technologischen Herausforderungen von Big Data hängen von unternehmensspezifischen Faktoren (Grösse, Branche, Ziele, etc.) ab. Viele Big-Data-Technologien sind als Open-Source-Lösungen verfügbar. Die eingesetzte Technologie muss die Transparenz über Datenströme, Bereinigungs- und Auswertungs-Aktivitäten, den Zugriff zu den richtigen Daten sowie einen ausreichenden Datenschutz ermöglichen (Zacher, 2012). Das Zusammenführen von (stark) disparaten Datenquellen sowie die Konsolidierung und Verknüpfung von strukturierten und unstrukturierten Daten sind nach wie vor schwierig und auch problematisch (Daten-Kontext).

## 2.4 Ökonomische Aspekte

Im Rahmen der Open-Data-Bewegung wird der freie Zugang zu Daten gefordert, um Dritten die Weiterverwendung und Weiterentwicklung von Daten zu ermöglichen. Dabei werden Daten und Informationen im weiteren Sinne als Infrastrukturgüter betrachtet (OECD 2015). Diese zeichnen sich dadurch aus, dass sie als Inputs für viele verschiedene Produktionsprozesse dienen können und ihr Konsum zumindest bis zu einem gewissen Grad nicht-rival ist (d.h. sie werden durch den Konsum nicht "verbraucht"). Die wirtschaftliche und gesellschaftliche Nachfrage nach Infrastrukturgütern geht in erster Linie auf die nachgelagerten Aktivitäten von Produktion und Konsum zurück, bei denen es sich zumindest teilweise um öffentliche und um nicht-marktwirtschaftliche Güter handelt, welche für die Gesellschaft positive Externalitäten generieren. Zu den traditionellen Infrastrukturgütern gehören Verkehrs- und Kommunikationsnetze, Bildungssysteme sowie Energie- und Wasserversorgungssysteme. Verschiedene weitere Ressourcen, welche traditionell nicht zu den Infrastrukturgütern gerechnet werden, haben sehr ähnliche Eigenschaften: Natürliche Ressourcen, Informationsressourcen, das Internet, usw. Aus einer ökonomischen Perspektive betrachtet, weisen Infrastrukturressourcen eine Reihe von Herausforderungen auf: Der relativ grosse Aufwand, jemanden von der Nutzung auszuschliessen (man denke beispielsweise an die Nutzung von Strassen), und bedeutende Skaleneffekte (natürliche Monopole) führen dazu, dass der Markt versagt und Infrastrukturgüter in zu geringem Ausmass produziert werden, wenn die Produktion allein dem Markt überlassen wird. Hinzu kommt, dass bedeutende positive Externalitäten beim Konsum (z.B. im Bereich der Bildung oder bei Hygienemassnahmen) es schwierig machen, den gesellschaftlichen Gesamtnutzen von Infrastrukturgütern zu eruieren, da der klassische Preismechanismus versagt. Hinzu kommt, dass Infrastrukturgüter oftmals mit bedeutenden Netzwerkeffekten (der Nutzen steigt mit einer zunehmenden Zahl von Nutzern) und Verbundeffekten (effizientere Produktion durch Mehrfachnutzung von Ressourcen) einhergehen (Frischmann 2005).

## 3 Methodologisches Vorgehen

Um die Chancen und Risiken von Big Data aus Sicht verschiedener Stakeholdergruppen in der Schweiz zu identifizieren und um unterschiedliche Sichten bezüglich der künftigen Data-Governance herauszuarbeiten, wurden zunächst mit Experten aus Wirtschaft, Verwaltung und Zivilgesellschaft leitfadengestützte Interviews durchgeführt. Die Ergebnisse wurden im Rahmen eines Workshops zur Weiterentwicklung der Strategie Informationsgesellschaft Schweiz und anlässlich des Swiss Internet Governance Forums 2015 vorgestellt und diskutiert. Um die gewonnenen Ergebnisse empirisch breiter abzustützen, zu ergänzen und durch Zahlen zu hinterlegen, wurde anschliessend eine quantitative Erhebung durchgeführt. Zielgruppe waren Personen in der Schweiz, welche sich mit Fragen rund um Big Data auseinandersetzen.

### 3.1 Fragestellungen und Modalitäten der Expertenbefragung

Bei der Expertenbefragung standen die folgenden Forschungsfragen im Vordergrund:

- Welches sind die Chancen, Risiken und Herausforderungen im Zusammenhang mit Big Data aus Sicht verschiedener Stakeholdergruppen in der Schweiz?
- Welche Ansichten und Vorstellungen bestehen bezüglich der aktuellen und künftigen Data-Governance?

Um diesen Fragen nachzugehen wurden im Frühjahr 2015 mit 20 Experten aus Wirtschaft, Verwaltung und Zivilgesellschaft leitfadengestützte Interviews zu den folgenden Themenfeldern durchgeführt:

- Bedeutung von Big Data: Chancen und Risiken
- Daten und Datenzugang
- Ethischer Umgang und Reputation
- Gesellschaftliche Aspekte
- Wandel der Organisationen
- Handlungsrichtlinien
- Technologische Herausforderungen

Dabei wurde zwischen zwei Kategorien von Interview-Partnern unterschieden, für die je ein Leitfaden in unterschiedlicher Ausprägung ausgearbeitet wurde:

- Beobachter von Big Data, welche Big Data nicht selber einsetzen
- Big-Data-Akteure, welche Big Data selber einsetzen, oder dies in Zukunft zu tun gedenken

Die beiden Leitfäden sind im Anhang zu finden (Anhänge 1 und 2).

Tabelle 1 enthält eine Kategorisierung der befragten Personen sowie die Angabe, welchen Organisationen sie angehören. Bei den privatwirtschaftlichen Big-Data-Akteuren sind folgende Branchen vertreten: Detailhandel, Online-Handel, Krankenversicherung, Telekommunikation, Pharmaindustrie und Transport. Hinzu kommen aus dem öffentlichen Sektor die Schweizerische Unfallversicherung sowie das Bundesamt für Statistik. Bei den Big-Data-Beobachtern wurden vor allem zivilgesellschaftliche Akteure befragt, wie die Stiftung Konsumentenschutz, der Verein Grundrechte, der Verein open-data.ch, zwei Rechtsanwälte, ein Journalist, ein ehemaliger Journalist und Blogger sowie ein kantonaler Datenschützer. Ergänzt wurde die beobachtende Perspektive auf Big Data durch die Sicht von Vertretern der Melde- und Analysestelle Informationssicherung MELANI und der Betreiberin des Wissenschaftsnetzes der Schweizer Hochschulen SWITCH.

Was die Rolle der Interviewpartner innerhalb ihrer Organisationen anbelangt, so wurden bei den Akteuren mit Big Data Personen aus ganz unterschiedlichen Aufgabenbereichen befragt, wie Business

Information Management / Business Intelligence, Kommunikation/Marketing, Data Science, Controlling, Public Policy sowie Business Development.

	Zivilgesellschaft	Verwaltung / Hochschulen	Privatwirtschaft
Big-Data-Beobachter	Stiftung Konsumentenschutz Verein Grundrechte Verein opendata.ch 2 Rechtsanwälte 1 Journalist 1 Ehem. Journalist und Blogger 1 Datenschützer	MELANI SWITCH	N/A
Big-Data-Akteure	<i>Persönliche Einschätzungen einzelner Vertreter der Privatwirtschaft</i>	BFS Suva	Coop CSS Digitec/Galaxus Migros Ricardo Roche SBB UPC-Cablecom

Tabelle 1: Interview-Partner nach Kategorien

### 3.2 Fragestellungen und Modalitäten der quantitativen Erhebung

Mit der quantitativen Erhebung wurde einerseits das Ziel verfolgt, die Ergebnisse der Experten-Interviews zu quantifizieren und gemäss den verschiedenen Stakeholder-Gruppen aufzuschlüsseln. Ausserdem sollten zusätzlich zu den Chancen und Risiken von Big Data auch die Bereiche identifiziert werden, in denen kollektiver Handlungsbedarf besteht, und im Speziellen der Handlungsbedarf des Bundes aufgezeigt werden. Demnach standen die folgenden Forschungsfragen im Vordergrund:

- Welche Bedeutung hat Big Data für die verschiedenen Stakeholder-Gruppen?
- Welches sind die Chancen und Risiken aus Sicht der verschiedenen Stakeholder-Gruppen?
- Welche Ansichten und Vorstellungen hegen die Befragten hinsichtlich Datenschutz und Data Governance?
- In welchen Bereichen besteht im Zusammenhang mit Big Data kollektiver Handlungsbedarf? (Hierzu wurden ausgehend von den Ergebnissen der Experten-Interviews eine Reihe von konkreten Fragen formuliert – siehe Tabelle 2.)
- In welchen Bereichen und in welcher Form sollte die öffentliche Hand aktiv werden? Welches ist im Speziellen der Handlungsbedarf des Bundes?

Der Fragebogen wurde basierend auf den durch die Interviews und im Rahmen der anschliessenden Diskussion der Ergebnisse gewonnenen Erkenntnissen entwickelt und unter Beizug von Personen aus der Zielgruppe getestet (der Fragebogen ist in Anhang 3 zu finden).

Die quantitative Erhebung fand im Juni 2015 in Form einer Online-Befragung auf Deutsch und Französisch statt. Als Zielgruppe im Fokus standen Personen in der Schweiz, welche in ihrem Alltag mit Big Data in Berührung kommen bzw. sich dazu Gedanken machen – sei es im Rahmen ihrer beruflichen Tätigkeit, ihrer politischen Aktivitäten oder privat. Rund 2700 Einzelpersonen und 140 Organisationen wurden direkt angeschrieben, wobei es bei der Kontaktnahme mit den Organisationen darum ging, eine geeignete Person innerhalb der Organisation zur Teilnahme an der Umfrage zu bewegen und nicht darum, eine offizielle Stellungnahme der Organisation einzuholen. Ergänzend wurden Mitglieder bestimmter Gruppen (z.B. die Mitglieder der Open Data Community oder Personen, welche sich für den Schutz der Privatsphäre einsetzen) über einen „Open Call“ via Mailinglisten zur

Teilnahme eingeladen. Die direkt Angeschriebenen erhielten zusätzlich zur Einladungsmail im Abstand von ca. 10 Tagen zwei Erinnerungsmails, sofern sie den Fragebogen bis dahin noch nicht ausgefüllt hatten.

<p><b>Internationale Dimension</b></p> <p>In welchen Bereichen ist die Souveränität der Schweiz <i>de facto</i> beschränkt?</p> <p>In welchen Bereichen ist eine internationale Koordination erwünscht bzw. unabdingbar?</p> <p>Welche internationale Governance-Architektur ist zweckmässig?</p>	<p><b>Regulatorische Massnahmen</b></p> <p>Welche neuen gesetzlichen Vorgaben braucht es?</p> <p>In welchen Bereichen braucht es allgemeinverbindliche Standards?</p> <p>In welchen Bereichen braucht es veränderte Aufsichtsrollen?</p>
	<p><b>Anreizsysteme / Flankierende Massnahmen</b></p> <p>Welche Aufklärungs- und Sensibilisierungsmassnahmen braucht es?</p> <p>Welche Akzente sind bei der Aus- und Weiterbildung zu setzen?</p> <p>Welche Massnahmen braucht es im Bereich der Innovationsförderung?</p>
	<p><b>Verwaltungstätigkeit</b></p> <p>Welche Anpassungen braucht es hinsichtlich der Datenproduktion und der Datenbereitstellung durch Behörden?</p> <p>Welche Anpassungen braucht es im Bereich der Datennutzung durch Behörden?</p>

Tabelle 2: Staatliche Handlungsfelder / Bereiche, in denen kollektiver Handlungsbedarf bestehen könnte

## 4 Bedeutung von Big Data für Wirtschaft und Gesellschaft

### 4.1 Bedeutung von „Big Data“ aus Sicht der befragten Personen

Da der Term „Big Data“ bisweilen unterschiedlich definiert wird, wurden im Rahmen der qualitativen Befragung die Interview-Partner eingangs des Gesprächs gefragt, was sie unter „Big Data“ verstehen. Tabelle 3 gibt einen Überblick über die am häufigsten genannten Aspekte von Big Data. Dazu gehören die in der Literatur gemeinhin angeführten drei „V“ – also „Volume“, „Variety“ und „Velocity“ sowie die Verwendung neuer Analyse-Methoden (wie Mustererkennung oder die Suche nach Algorithmen). Mehrere Interview-Partner wiesen aber darauf hin, dass es sich bei der Analyse von grossen Datenmengen nicht um etwas grundsätzlich Neues, sondern um einen allmählichen Trend infolge grösserer Analyse- und Speicherkapazitäten handelt.

Akteure mit Big Data	Big-Data-Beobachter
<b>Volume:</b> grosse Mengen von Daten bzw. immer mehr Daten werden verarbeitet. Dabei handelt es sich um einen <b>allmählichen Trend infolge von verbesserten technischen Möglichkeiten</b> (grössere Analyse- und Speicherkapazitäten) und nicht um etwas grundsätzlich Neues.	
<b>Variety:</b> es werden Daten aus verschiedenen Beständen verknüpft und vernetzt; dies hat zur Folge, dass unterschiedlich strukturierte Daten in vielen verschiedenen Formaten aus verschiedenen Quellen verarbeitet werden.	
<b>Velocity:</b> Es kommt zu einer immer schnelleren Verarbeitung von Daten.	<b>Neue Analyse-Methoden:</b> Big Data wird von neuen Daten-Analyse-Modellen begleitet (Mustererkennung, Suche nach Algorithmen).

Tabelle 3: Bedeutung von „Big Data“ aus Sicht der befragten Personen

### 4.2 Die Rolle von Big Data in den befragten Unternehmen

Die im Rahmen der qualitativen Erhebung befragten Unternehmen befinden sich mit Blick auf den Einsatz von Big Data in ganz unterschiedlichen Entwicklungsstadien. Während die einen bereits über eine eigene Abteilung mit spezialisiertem Personal verfügen, die sich um Big Data kümmert, haben andere erst kürzlich ein Projekt oder eine Arbeitsgruppe eingesetzt, die sich mit der Thematik befasst und abklären soll, wie Big Data im jeweiligen Unternehmen am besten eingesetzt werden kann. Zwei der befragten Unternehmen verfügen aktuell noch über keine Big-Data-bezogenen Aktivitäten, können sich den Einsatz von Big Data in Zukunft aber vorstellen.

Die meisten befragten Unternehmen verwenden vor allem Daten, welche direkt im Rahmen ihrer Geschäftstätigkeit anfallen. Punktuell werden auch externe Daten verwendet. Teilweise werden auch Daten weitergegeben, jedoch kaum Personendaten und dann meist nur in aggregierter Form.

### 4.3 Chancen von Big Data

Tabelle 4 enthält eine Übersicht über die am häufigsten genannten Chancen von Big Data. Die von den Akteuren wie auch von den Beobachtern am häufigsten genannte Chance von Big Data ist das Gewinnen neuer Erkenntnisse und Entdecken neuer Zusammenhänge durch Kombination von verschiedenen Datenbeständen und dank besseren Analysemöglichkeiten. Hinzu kommen die Personalisierung von Angeboten, Informationen und Werbung sowie verbesserte Prognosen ganz unterschiedlicher Art, sei es im operativen Geschäft (Materialausfälle), bei der Unfallprävention, der Prävention von Betrugsfällen, der Verbrechensbekämpfung oder zur Vorhersage von klimatischen Veränderungen. Weitere Chancen, die von Akteuren mit Big Data genannt wurden, sind die erhöhte

Agilität dank Real-Time-Auswertungen sowie die Tatsache, dass dank besseren Datenauswertungen vermehrt faktenbasierte Entscheide getroffen werden können.

Akteure mit Big Data	Big-Data-Beobachter
Gewinnen neuer <b>Erkenntnisse</b> und Entdecken neuer Zusammenhänge dank Kombination und besserer Analyse von Daten	
<b>Personalisierung / Tailoring</b> von Angeboten, Informationen, Werbung	
Verbesserte <b>Prognosen</b> (z.B. Ausfälle von operativem Material, Unfälle, Betrugsfälle, Verbrechen, Kreditausfälle, klimatische Veränderungen)	
<b>Agilität</b> dank Real-Time-Auswertungen	
Vermeehrt <b>faktenbasierte Entscheide</b> (im Gegensatz zur Orientierung an Erfahrungswissen und Intuition)	

Tabelle 4: Die meistgenannten Chancen von Big Data

Die Big-Data-Beobachter wurden überdies gefragt, welche Branchen aus ihrer Sicht am ehesten von Big Data profitieren. Dabei wurden die folgenden Branchen am häufigsten genannt (Mehrfachnennungen):

- Daten-Sammel-Firmen als Intermediäre z.B. für Werbetreibende, wie Google, Amazon oder Facebook
- Krankenkassen / Versicherungen (verfeinertes Risikomanagement)
- Finanzintermediäre (Banken, Versicherungen)
- Werbeindustrie, Marketing, Anbieter von Produkten und Dienstleistungen
- Medizinische und biologische Forschung, Pharmaunternehmen

Weitere Bereiche, die in diesem Zusammenhang von einzelnen Interview-Partnern genannt wurden, sind die Weltraumforschung, Post und Logistik, Telekomunternehmen, die Produktionsindustrie (Fertigungsdaten), Online-Shops (dynamisches Pricing), Politik und Verwaltung (bessere Entscheidungen) sowie kleine, hochspezialisierte Nischenmärkte. Es wurde allerdings von mehreren Personen angemerkt, dass hinsichtlich der Verwendung von Big Data der Phantasie keine Grenzen gesetzt sind und dass nicht jede Verwendung nach aussen hin auch kommuniziert wird. Im Gegenteil: Es ist davon auszugehen, dass bestimmte Unternehmen versuchen werden, ihre Nutzung von Big Data so lange wie möglich geheim zu halten. Aus diesem Grund ist das hier gezeichnete Bild nicht unbedingt verlässlich.

#### 4.4 Risiken und Herausforderungen im Zusammenhang mit Big Data

Den Chancen stehen Risiken und Herausforderungen gegenüber. Die meistgenannten sind in der Tabelle 5 ersichtlich. Hier zeigte sich im Laufe der Expertenbefragung, dass ein breiter Konsens besteht, dass die Datenschutzproblematik bzw. die Gefahr des Datenmissbrauchs im Zusammenhang mit der Nutzung von Big Data die grösste Herausforderung darstellt. Es scheint unbestritten, dass mit Big Data nicht nur die Wahrscheinlichkeit von Missbräuchen zunimmt, sondern auch das Schadenspotential steigt.

Mit der Thematik des Datenmissbrauchs verbunden sind auch die erhöhte Manipulationsgefahr und die grundsätzliche Bedrohung der Privatsphäre, welche einige der befragten Personen ausmachen. Für die Unternehmen, welche Big Data einsetzen, bestehen neben dem Risiko von Datenmissbrauch durch eigene Mitarbeitende oder Dritte, die sich unrechtmässigerweise Zugang zu den Daten verschaffen, auch Image-Risiken bei vermuteten oder empfundenen Datenschutzverletzungen. Dies auch in Fällen, in denen die gesetzlichen Vorgaben und vertraglichen Bestimmungen klar eingehalten wurden. Hier

geht es daher immer auch darum, über die rechtlichen Überlegungen hinaus abzuschätzen, welche Verwendung der Daten von Kunden und Benutzern als zu intrusiv empfunden wird und daher auf Ablehnung stossen könnte.

Akteure mit Big Data	Big-Data-Beobachter
<b>Datenschutzproblematik / Datenmissbrauch</b>	
<b>Image-Risiken</b> bei vermuteten oder empfundenen Datenschutzverletzungen (trotz Einhaltung der gesetzlichen Vorgaben)	<b>Manipulationsgefahr</b>
	<b>Grundsätzliche Bedrohung der Privatsphäre</b>
<b>Erhöhte Kunden-/Auftraggeber-Erwartungen</b> hinsichtlich datenbasierter Zusatzdienste	<b>Fehlender Datenzugang:</b> <i>Personenunabhängige</i> Daten sollten im Sinne von Open Data offen sein; viele dieser Daten sind heute nicht zugänglich
Da noch <b>keine standardisierten Tools</b> vorliegen, sind <b>bedeutende Investitionen</b> nötig	<b>Datenmonopole; Ungleichheiten und soziale Ungleichgewichte</b> bezüglich der Verfügung über Daten und deren Nutzung
Verschiedene Unternehmen bekunden <b>Mühe, Business Cases für einen rentablen Einsatz von Big Data zu finden</b>	<b>Mangelndes Bewusstsein der Bürger / Nutzer</b> , wie Daten genutzt werden (können)

Tabelle 5: Die meistgenannten Risiken und Herausforderungen von Big Data

Des Weiteren wurden seitens der befragten Unternehmensvertreter auch erhöhte Kunden- und Auftraggebererwartungen hinsichtlich datenbasierter Zusatzdienste angeführt. Mehrere Befragte empfinden es als schwierig, angesichts gesteigerter Erwartungen in Richtung personalisierter Dienste einerseits und berechtigter Datenschutzbedenken andererseits allen Ansprüchen gerecht zu werden. Man verspürt in gewissen Fällen intern keinen grossen Drang, Big Data einzusetzen, fürchtet aber, dass der Zug für die eigene Organisation plötzlich abgefahren ist, wenn man sich nicht frühzeitig mit der Thematik auseinandersetzt. Und schliesslich bekunden verschiedene Unternehmen Mühe, Anwendungsmöglichkeiten für einen rentablen Einsatz von Big Data zu finden, was teilweise damit zusammenhängen dürfte, dass derzeit noch kaum standardisierte Tools für den Umgang mit Big Data vorliegen und die Unternehmen daher bedeutende Investitionen tätigen müssen, bevor sie in diesem Feld überhaupt aktiv werden können. Daneben gibt es aus Sicht von Big-Data-Beobachtern aber auch kulturelle Barrieren, die sich darin äussern, dass viele Organisationen heute gar noch nicht darauf eingestellt sind, Daten aus eigenen und fremden Quellen im Sinne einer Sekundärnutzung weiterzuverwenden.

Eine weitere wichtige Herausforderung, die von verschiedenen Big-Data-Beobachtern genannt wurde, ist der fehlende Zugang zu vielen Daten, deren Weiterverwendung einen gesellschaftlichen Nutzen stiften könnte. Hier könnte eine konsequente Anwendung des Open-Data-Prinzips auf alle personenunabhängigen Daten Abhilfe schaffen. Aus den Aussagen von Akteuren mit Big Data zu schliessen, geht es aber nicht nur um den freien Zugang zu den Daten, sondern die Daten müssen auch in hinreichender Qualität vorhanden sein, was heute oftmals nicht der Fall sei. Zudem muss ihre Verfügbarkeit in gewissen Anwendungsfällen über mehrere Jahre hinweg garantiert werden können (z.B. Referenzwerte bei offiziellen Statistiken, die in regelmässigen Abständen aktualisiert werden). Staatliche Akteure weisen zudem auf rechtliche Grauzonen beim Zukauf von Daten aus der Privatwirtschaft hin.

Als weitere Herausforderungen werden seitens der Big-Data-Beobachter auch ökonomische Aspekte angeführt, wie Datenmonopole oder generell Ungleichheiten und soziale Ungleichgewichte bezüglich der Verfügung über Daten und deren Nutzung. Zu ökonomischen Ungleichgewichten führt auch das mangelnde Bewusstsein der Bürger und Nutzer darüber, wie ihre Daten genutzt werden bzw. genutzt werden könnten. Hier wird auch die weitgehende Intransparenz hinsichtlich der tatsächlichen Nutzung

der Daten bemängelt, die dazu führt, dass die Nutzer gegenüber von Unternehmen, die ihre personenbezogenen Daten sammeln, eine schwache Verhandlungsposition innehaben.

Und schliesslich fördert die Diskussion von Problemfeldern auch zwiespältige Aspekte von Big Data zutage. So wird die Personalisierung von Angeboten, Werbung und Informationen von vielen Menschen zumeist als positiv empfunden. Sie kann aber in gewissen Fällen auch das Gefühl hervorrufen, dass man ausspioniert wird, so dass bei personalisierten Angeboten die Eingriffe in die Privatsphäre bisweilen als störend empfunden werden. Auch personalisierte Preisdifferenzierungen bei Käufen im Internet werden von den befragten Big-Data-Beobachtern als Problem gesehen. Des Weiteren birgt eine exzessive Personalisierung von Informationen und Angeboten die Gefahr, dass sich die Leute nicht mehr für neue Dinge interessieren, da sie sich dauernd in einer vorgefilterten Welt bewegen.

Umstritten ist auch das Argument, dass Big Data positiv sei, da es vermehrt faktenbasierte Entscheide ermögliche und man sich dadurch weniger häufig allein auf sein Bauchgefühl verlassen müsse. Dem entgegen andere, dass Big Data durchaus auch die Gefahr birgt, dass man sich zu sehr auf Daten und zu wenig auf sein unternehmerisches Gespür verlässt. Man sollte sich bewusst sein, dass die Daten immer zurückschauen und sich vor allem zur Analyse von relativ statischen Systemen eignen. Erfolgreiches wirtschaftliches Handeln beinhaltet aber auch, Trends zu setzen, und dazu sei die Analyse von Daten aus der Vergangenheit denkbar ungeeignet.

#### 4.5 Herausforderungen, um Big Data in Unternehmen und Organisationen zu valorisieren

Die Akteure mit Big Data wurden zusätzlich auch ganz konkret nach den Herausforderungen bei der Valorisierung von Big Data innerhalb ihres Unternehmens bzw. ihrer Organisation gefragt. Dabei wurden die folgenden Aspekte am häufigsten genannt:

- **Kulturwandel:** Der Wechsel hin zu einem neuen Paradigma im Umgang mit Daten und bei der Entscheidungsfindung stellt viele Organisationen vor bedeutende Herausforderungen. Es geht darum, die verschiedenen Akteure innerhalb der Organisation dazu zu bringen, vermehrt datenbasiert zu entscheiden, und zugleich die Bereitschaft für ein experimentelles Vorgehen zu fördern. Im Endeffekt müssen die Organisationen agiler werden, um wirklich von Big Data profitieren zu können.
- **Nutzen / Rentabilität von Big Data aufzeigen und erzielen:** Der Einsatz von Big-Data-Technologien erfordert bei den Unternehmen beträchtliche Investitionen in die Infrastruktur. Dadurch besteht ein hoher Druck, aus der Anwendung dieser Technologie auch tatsächlich einen geschäftlichen Nutzen zu ziehen. Dieser entsteht aber erst durch das Zusammenspiel zwischen den Daten-Analysten und den einzelnen Geschäftsbereichen. Erst wenn die einzelnen Geschäftsbereiche den vorgängig beschriebenen Kulturwandel durchmachen, wird der potentielle Nutzen von Big Data im Unternehmen Realität. Die befragten Unternehmen tun sich teilweise schwer damit, überhaupt Business Cases zu finden, welche die getätigten bzw. die zu tätigenden Investitionen legitimieren würden. Hinzu kommt, dass Big-Data-Projekte, die im Kern neue Erkenntnisse zum Ziel haben (im Gegensatz zu Projekten, die eine Optimierung bestehender Prozesse anstreben) nach Aussage eines der befragten Experten mit rund 85% eine hohe Misserfolgsrate aufweisen.
- **Kompetenzaufbau und -diffusion:** Der Einsatz von Big Data erfordert neue Kompetenzen, die in den Unternehmen oftmals noch nicht vorhanden sind. Zum einen muss spezifisches Know-how aufgebaut werden, was die Analyse von Einzeldaten (im Gegensatz zu Aggregatsdaten) anbelangt; zum anderen braucht es Leute, welche die Brücke bauen zwischen Statistikern und Technikern und den Fachabteilungen. Dabei besteht die organisationale Herausforderung darin, das Know-how einerseits zu zentralisieren und andererseits dezentral in eigenständigen Fachprozessen zur Wirkung zu bringen. Mehrere der befragten Unternehmen wiesen darauf hin, dass sie die Einführung von Big Data schrittweise angehen (nach und nach werden immer mehr und immer aktuellere Daten analysiert) und dass sie es den Beteiligten im Rahmen von überschaubaren Pilotprojekten ermöglichen, gemeinsam den Umgang mit Big Data zu erlernen.
- **Datenschutz:** Hinsichtlich des Datenschutzes besteht die Herausforderung einerseits darin, dass man den Daten-Analysten einen möglichst umfassenden Zugang zu teilweise sensiblen Daten gewähren muss. Andererseits braucht es bisweilen sehr viel Fingerspitzengefühl, um

über die Anwendung der gesetzlichen und reglementarischen Vorgaben hinaus abzuschätzen, welche Datenanalysen von den Kunden geschätzt bzw. toleriert werden und welche auf eine Ablehnungshaltung stossen und damit zu einem Reputationsschaden führen könnten. Hier steht zu erwarten, dass es auch zu ethischen Spannungsfeldern zwischen dem Machbaren und dem Wünschbaren kommt, mit denen man sich intern auseinandersetzen muss.

- **Datenqualität:** Die Überprüfung der Datenqualität gestaltet sich bisweilen schwierig. Grundsätzlich gilt: je strukturierter die Daten und je näher sie am Business sind, desto höher ist die Qualität. Das Zusammenziehen von Daten unterschiedlicher Qualität aus heterogenen Quellen funktioniert bei Anwendungen, bei denen die 80/20-Regel angewendet werden kann, ganz gut. Bei höheren Qualitätsansprüchen ist es schwierig, an geeignete Daten heranzukommen.
- **Technische Herausforderungen:** Die genannten technischen Herausforderungen bestehen in erster Linie darin, geeignete Software und Hardware anzuschaffen, die sich für die schnelle Verarbeitung von grossen Datenmengen eignet. Zudem wird im Bereich der Infrastruktur im Zusammenhang mit Big Data eine hohe Erneuerungsrate konstatiert, da laufend mehr Daten und Datenquellen hinzukommen und der schnelle Wandel bei den eingesetzten Softwarelösungen dazu führt, dass häufig neue Lösungen getestet und möglicherweise eingeführt werden müssen. Um bei diesem schnellen technologischen Wandel mithalten zu können, braucht es ein relativ grosses Technologiewissen und eine gute Kenntnis des Ökosystems.

## 5 Grundlagen der Data Governance auf gesellschaftlicher Ebene

Im Rahmen dieser Studie definieren wir „Data Governance“ als Set von Regeln, Entscheidungsbefugnissen und Rechenschaftspflichten, durch die festgelegt wird, wer mit welchen Informationen, wann und unter welchen Bedingungen unter Verwendung welcher Methoden welche Handlungen ausführen darf bzw. muss<sup>2</sup>. Dabei fokussieren wir nicht auf die Data Governance innerhalb eines Unternehmens, sondern auf die Data Governance auf gesamtgesellschaftlicher Ebene. Ziel der Data Governance auf gesellschaftlicher Ebene ist es, die Gesetze und Regeln hinsichtlich der Bereitstellung, Pflege und Nutzung von Daten und Informationen so auszurichten, dass bei möglichst geringen Risiken der grösstmögliche gesellschaftliche Nutzen erzielt wird.

Im Rahmen der Expertenbefragung wurden verschiedene Aspekte thematisiert, welche die Data Governance mehr oder weniger direkt betreffen. Das vorliegende Kapitel enthält einen Überblick über die wichtigsten Ergebnisse, während in Kapitel 5 darauf aufbauend sieben Thesen im Hinblick auf eine „Good“ Data Governance formuliert werden.

### 5.1 Daten-Typologie als Grundlage für eine sinnvolle Data Governance

Wenig überraschend sind sich die befragten Personen weitgehend einig, dass zwischen verschiedenen Arten von Daten unterschieden werden muss. Dabei können folgende Kriterien als Grundlage einer sinnvollen Data Governance dienen:

Angesichts der Tatsache, dass der Schutz von personenbezogenen Daten im Zusammenhang mit Big Data eine der grössten Herausforderungen darstellt, liegt es auf der Hand, dass zunächst zwischen **personenbezogenen Daten** und **nicht-personenbezogenen Daten** unterschieden wird. Es besteht ein breiter Konsens darüber, dass für diese beiden Typen von Daten unterschiedliche Regeln gelten sollten.

Folgt man der Argumentation der Open-Data-Bewegung, sollten alle Daten der öffentlichen Hand zur freien Weiterverwendung verfügbar gemacht werden, welche keinen Einschränkungen hinsichtlich **Urheberrecht, Sicherheit, Privatsphäre** oder **Geschäftsgeheimnissen** unterliegen. Darüber hinaus wird bisweilen gefordert, dass alle **transparenzrelevanten Daten** im Internet publiziert werden sollten, also sämtliche Daten, welche bei politischen Entscheiden bzw. bei Behördenentscheiden eine wichtige Rolle spielen. Dies gilt sowohl für Behördendaten als auch für privatwirtschaftliche Daten. Ein in diesem Zusammenhang genanntes Beispiel betrifft die Veröffentlichung der Daten aus den Studien, welche bei Medikamentenzulassungen als Entscheidungsgrundlage beigezogen werden.

Bei den personenbezogenen Daten gehen die Ansichten auseinander: Während die einen fordern, dass Instrumente geschaffen werden, die es jedem Einzelnen ermöglichen, unter Beibehaltung einer möglichst grossen Kontrolle über die eigenen Daten auch personenbezogene Daten freizugeben, und die breite Freigabe solcher Daten für die Weiterverwendung (z.B. für die Gesundheitsforschung) als erstrebenswertes Ziel ansehen, gibt es andere, die monieren, dass die allzu breite Preisgabe von personenbezogenen Informationen der Gesellschaft schaden kann, da die Nutzung entsprechender Daten nicht nur in guter Absicht geschieht.

### 5.2 Verfügbarkeit der Daten

Die breite Verfügbarkeit von Daten wird grundsätzlich positiv bewertet, da sie zu einer Reihe von Vorteilen führe, wie:

<sup>2</sup> In Anlehnung an die Definition des Data Governance Institute, eines privaten Dienstleisters, der sich für die Belange der Data-Governance spezialisiert: *“Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.”*  
([http://www.datagovernance.com/adq\\_data\\_governance\\_definition/](http://www.datagovernance.com/adq_data_governance_definition/))

- Verbesserte Informationsmöglichkeiten
- Verbesserte Transparenz politischer Prozesse
- Geringere Manipulierbarkeit der Menschen
- Erkenntniszuwachs, schnellere Fortschritte in der Forschung
- Vorhersage von Gefahrensituationen, klimatischen Veränderungen usw.
- Entwicklung von neuen Produkten und Dienstleistungen

Zudem wird die breite Verfügbarkeit von Daten als Voraussetzung für die Konkurrenzfähigkeit der Schweizer Unternehmen und allgemein der Schweiz als Standort betrachtet. Von einem der Gesprächspartner wurde zudem angemerkt, dass eine Überflutung von Daten über die Schweiz aus dem Ausland drohe, wenn diese in der Schweiz nicht verfügbar sind. Dies könne zu einem Verlust der Datenautonomie führen.

Nachteile aus der breiten Verfügbarkeit von Daten ergeben sich vor allem im Bereich der Privatsphäre und im Zusammenhang mit der missbräuchlichen Verwendung von Daten. Hier wird im Zusammenhang mit Big Data sowohl eine erhöhte Missbrauchsgefahr als auch ein erhöhtes Schadenspotential konstatiert.

Die meisten befragten Unternehmen verwenden vor allem Daten, welche direkt im Rahmen ihrer Geschäftstätigkeit anfallen. Bei diesen Daten ist die Qualität in der Regel am höchsten und der Integrationsaufwand am geringsten. Viele der Befragten erachten das aktuelle Datenangebot vorerst als ausreichend, da heute die bestehenden Möglichkeiten hinsichtlich der Datenanalyse noch nicht ausgereizt werden. Einige machen sich aber durchaus Gedanken über die Einbindung weiterer Daten – sowohl aus internen als auch aus externen Quellen.

Zum Teil werden heute schon Daten von Dritten bezogen. Genannt wurden beispielsweise Geodaten für die Standortplanung von Detailhandelsgeschäften, Daten über Laufwege von Konsumenten und GfK-Marktdaten. Weitere Daten, die von einzelnen Unternehmen/Organisationen extern bezogen werden, sind Bonitätsdaten, Scannerdaten von Detailhandelsunternehmen sowie Daten von Behörden und bundesnahen Betrieben.

Des Weiteren wurde von einzelnen Befragten der Wunsch geäussert, in Zukunft (weitere) externe Daten zu beziehen. Konkret genannt wurden hierbei Wetterdaten, standardisierte Adressdaten (idealerweise als Open Data), Marktdaten, Daten von sozialen Medien, Bewegungsdaten (Swisscom / Mobilfunk) sowie Firmenprofile (wie sie z.B. von Orell Füssli aufbereitet werden). Generell ist festzustellen, dass die Datennachfrage sehr heterogen ist, und der thematische Fokus von Unternehmen zu Unternehmen stark variiert. Daher kann diese Auflistung keinesfalls den Anspruch auf Vollständigkeit erheben.

Teilweise werden von den befragten Unternehmen und Organisationen auch Daten weitergegeben, jedoch kaum Personendaten und dann meist nur in aggregierter Form. Während bei der Datenweitergabe die Datenschutzvorkehrungen die grösste Herausforderung darstellen, kommen beim Datenbezug oftmals die fehlende Qualität, die ungenügende Kenntnis des Erhebungskontexts (Definition der untersuchten Einheit und Population; zugrundeliegende Konzepte und Messgrössen) sowie die Unsicherheit hinsichtlich des langfristigen Zugangs zu Daten Dritter erschwerend hinzu.

### 5.3 Schutz von Personendaten – Datenschutz im Umbruch?

Der Schutz von Personendaten wird nicht nur als grösste Herausforderung im Zusammenhang mit Big Data angesehen, sondern es kursieren bezüglich des Datenschutzes der Zukunft auch ganz unterschiedliche Vorstellungen. Nach den Aussagen vieler Befragter zu schliessen, befindet sich der Datenschutz heute in der Krise bzw. im Umbruch. Dabei können folgende Ansätze unterschieden werden:

- **Traditioneller Ansatz:** Gemäss dem traditionellen Ansatz, der auch die gängige Rechtslage widerspiegelt, sind Daten zu Gesundheit, finanzieller Situation, Religion, politischer Zugehörigkeit usw. besonders schützenswert. Nicht besonders schützenswert sind hingegen Daten, die sowieso öffentlich sind, wie Name, Wohnort, Alter oder Geschlecht.

- **Big-Data-orientierter Ansatz:** Im Gegensatz zum klassischen Ansatz werden beim Big-Data-orientierten Ansatz diejenigen Daten als besonders schützenswert angesehen, die es erlauben, jemanden zu identifizieren, denn diese Daten ermöglichen es, Personendaten aus unterschiedlichen Quellen miteinander zu verknüpfen. Gemäss dieser Sichtweise sind es nicht so sehr einzelne, besonders heikle Informationen, die um jeden Preis vertraulich bleiben müssen, sondern es wird vielmehr das Zusammenführen vieler verschiedener – auf den ersten Blick unter Umständen völlig harmloser – personenbezogener Informationen in einer digitalen Identität bzw. in einem Personenprofil als problematisch erachtet.
- **Relativistische Ansätze:** Im Rahmen der Befragung konnten zwei relativistische Ansätze identifiziert werden. Gemäss dem ersten variiert die Art der Daten, die als schützenswert betrachtet werden, individuell und ist auch kulturell geprägt. Gemäss dem zweiten Ansatz sollte immer kontextabhängig, hinsichtlich des Verwendungszwecks festgelegt werden, zu welchen Daten jemand Zugang hat. Beiden Ansätzen ist gemeinsam, dass sie eine generelle Unterscheidung zwischen besonders schützenswerten und weniger schützenswerten Daten ablehnen.
- **Ansatz der persönlichen Datenhoheit:** Der Ansatz der persönlichen Datenhoheit kommt in der Forderung zum Ausdruck, dass es in der Kontrolle jeder/jedes Einzelnen liegen sollte, welche Daten er/sie herausgeben möchte („It’s not about privacy, it’s about control!“). Dieser Ansatz ist mit den relativistischen Ansätzen kompatibel, setzt aber eine entsprechende Befähigung der Nutzerinnen und Nutzer und die Bereitstellung entsprechender Infrastrukturen voraus.
- **Ansatz der Unversehrtheit der digitalen Identität:** Gemäss diesem Ansatz ist die digitale Identität gleich zu schützen wie die physische; analog zur Garantie der physischen Unversehrtheit müssen auch die Daten, die eine Person betreffen, korrekt sein. Damit adressiert dieser Ansatz vor allem das Problem, dass Falschinformationen zu einer Person zu einer ungewollten Diskriminierung dieser Person durch Systeme führen können, die auf der Basis von Daten Entscheide fällen. Ein Paradebeispiel in diesem Zusammenhang sind die Personen, die im Anschluss an 9/11 fälschlicherweise auf den amerikanischen No-Fly-Listen figurierten.

Es dürfte ein Ding der Unmöglichkeit sein, alle diese Ansätze unter einen Hut zu bringen. Zudem gibt es beim Ansatz der persönlichen Datenhoheit ernsthafte Zweifel bezüglich der Umsetzbarkeit, denn er setzt nicht nur deutliche Fortschritte im Bereich der Human-Data-Interaction voraus, sondern erfordert vom Nutzer auch ein gewisses Niveau an Data-Literacy, während seine Position gegenüber der Marktmacht grosser Anbieter gestärkt werden müsste. Die grundsätzliche Frage besteht darin, wie man die Kontrollmöglichkeiten für den Einzelnen sicherstellt und den Otto-Normalverbraucher dazu befähigt, sowohl den Wert von Daten als auch die Risiken im Zusammenhang mit ihrer Preisgabe realistisch einzuschätzen. Zugleich lässt die breite Kritik am traditionellen Ansatz vermuten, dass es im Bereich des Datenschutzes in den nächsten Jahren zu einem Umbruch kommen könnte. Jedenfalls scheint angesichts der Brisanz der Thematik und der Heterogenität der vorgeschlagenen Ansätze eine breite gesellschaftliche Auseinandersetzung mit dieser Thematik angezeigt.

#### 5.4 Nutzerverhalten hinsichtlich der Preisgabe von personenbezogenen Daten

Die Befragten wurden nicht nur zum Datenschutz befragt, sondern auch zum Nutzerverhalten hinsichtlich der Preisgabe von personenbezogenen Daten. Hier lassen sich vier allgemeine Beobachtungen konstatieren:

- Es gibt einen **Generationenunterschied**. Dieser zeigt sich darin, dass die jüngere Generation viel freizügiger bzw. sorgloser mit persönlichen Daten umgeht als die ältere Generation.
- Es ist eine **zunehmende Sensibilisierung für Datenschutzbelange** zu beobachten. Grundsätzlich sind die Leute für Datenschutzbelange sensibilisierter, was sich aber nicht immer in ihrem Handeln widerspiegelt.
- Denn ebenso hat sich ein **Gewöhnungseffekt** bzw. eine gewisse **Resignation** eingestellt: Es ist in Datenschutzbelangen ein verstärktes Laisser-faire zu beobachten („so schlimm ist es ja nicht“); das Interesse an Geschäftsbedingungen nimmt ab. Doch das hat nicht unbedingt mit Desinteresse zu tun, sondern vielmehr damit, dass man bei den Nutzungsbedingungen von Online-Diensten oftmals keine echte Wahl hat: Entweder akzeptiert man die Bedingungen, die einem vorgelegt werden, oder man verzichtet ganz auf die Nutzung des jeweiligen Dienstes.

- **Die Online-Interaktionen haben in den letzten Jahren massiv zugenommen.** Eine wichtige Rolle spielt der weit verbreitete Einsatz von mobilen Geräten; es fallen dadurch immer mehr Personendaten an (wie z.B. Bewegungsprofile).

Bei der Interpretation dieser Beobachtungen gehen die Meinungen allerdings auseinander. Dabei betreffen die unterschiedlichen Bewertungen folgende Fragen:

- Erhalten die Leute für die Preisgabe ihrer Daten eine faire Gegenleistung oder werden sie von den Daten sammelnden Unternehmen über den Tisch gezogen?
- Pflegen die Digital Natives einen bewussteren Umgang mit ihren Daten oder verhalten sie sich aufgrund mangelnder Kenntnisse zu leichtfertig? Oder ist ganz einfach ihre Bereitschaft geringer, auf die positiven Aspekte zu verzichten? Oder ist gar der Preis höher, den sie bei einem Verzicht auf gewisse Online-Dienste bezahlen, über die heutzutage insbesondere zwischen jüngeren Menschen ein substantieller Teil der sozialen Interaktionen abgewickelt wird?
- Wem sollte ich meine Personendaten eher anvertrauen: dem Staat oder privaten Unternehmen? Wo ist das Missbrauchsrisiko grösser?
- Sollte jede Person selber entscheiden können, welche Daten sie über sich für welche Gegenleistung preisgeben möchte? Wäre die Freigabe von möglichst vielen Personendaten (z.B. zu Forschungszwecken) sogar ein erstrebenswertes Ziel? Oder ist es aus gesellschaftlicher Sicht problematisch, wenn viele Nutzer ihre persönlichen Daten aus individuellen Überlegungen heraus preisgeben?

## 5.5 Der Wert von Daten und wer davon profitiert

Was ist eine angemessene Gegenleistung beim Tausch von Privacy gegen eine Dienstleistung? – Während die befragten Unternehmen mit Kundenbindungsprogrammen der Ansicht sind, im Tausch für die Preisgabe von personenbezogenen Daten eine adäquate Gegenleistung zu erbringen, gehen die Ansichten bei den übrigen Befragten auseinander. Während sich die einen auf den Standpunkt stellen, dass man bei gewissen Dienstleistern (z.B. Google) im Gegenzug zur Preisgabe von persönlichen Daten eine beträchtliche Palette von Diensten nutzen kann, die man aus dem Alltag nicht mehr wegdenken möchte, haben andere das Gefühl, dass die Nutzer übervorteilt werden, und der tatsächliche Wert der preisgegebenen Daten viel höher ist als der Wert der bezogenen Leistungen.

Ebenso unterschiedlich wird der Mechanismus der Preisbildung bewertet: Während die einen davon ausgehen, dass im Bereich der Daten der Markt spielt und daher davon auszugehen ist, dass für personenbezogene Daten in der Regel in Form von Gegenleistungen ein fairer Preis bezahlt wird, wenden andere ein, dass der Markt im Bereich der Daten in eklatanter Weise versagt. Gründe dafür sind natürliche Monopole (infolge von Netzwerkeffekten) und Informations-Asymmetrien zwischen Unternehmen und Nutzern sowie negative Externalitäten (negative gesellschaftliche Effekte der Datenpreisgabe trotz positiven Effekten auf individueller Ebene). Mehrere der befragten Personen befürchten denn auch, dass mit der zunehmenden Verwendung von Big Data die sozialen und wirtschaftlichen Ungleichgewichte zunehmen, was in soziale Verwerfungen münden kann, wenn kein adäquater Ausgleich geschaffen wird.

## 5.6 Allgemeine technische bzw. methodologische Herausforderungen von Big Data

Die Data Governance muss sich an den technischen und methodologischen Möglichkeiten orientieren. Die Teilnehmer der qualitativen Befragung wurden daher auch nach den technischen Herausforderungen im Zusammenhang mit Big Data gefragt. Wenn es darum geht, die Chancen von Big Data besser wahrzunehmen und die Risiken zu mindern, stehen wir heute aus Sicht der Befragten vor den folgenden technischen bzw. methodologischen Herausforderungen:

- **Human-Data-Interaction:** Im Bereich der Human-Data-Interaction müssen technische Lösungen gefunden werden, welche die Nutzerinnen und Nutzer befähigen, informierte Entscheide über die Nutzung ihrer Daten zu fällen und einfach zum Ausdruck zu bringen. Die Entwicklung solcher Lösungen steht erst am Anfang, ist aber Voraussetzung für ein Empowerment der

Nutzerinnen und Nutzer, was die Weitergabe und Nutzung ihrer personenbezogenen Daten anbelangt.

- **Technische Datenschutzlösungen:** Es gilt Hardware- und Softwarelösungen zu entwickeln, welche den Datenschutz in der Architektur eingebaut haben. Dazu gehören beispielsweise technische Barrieren, die es verhindern, dass gewisse Daten miteinander kombiniert werden, die automatische Löschung von Daten oder physische Schranken (z.B. Speicherung von sensiblen Daten auf Systemen, welche nicht mit dem allgemeinen Firmennetzwerk verbunden sind). Aus Sicht mehrerer Befragter kann der Schutz von Personendaten heute nur noch mittels technischer Lösungen sichergestellt werden. Rechtliche und reglementarische Vorkehrungen allein reichen nicht aus.
- **Künstliche Intelligenz:** Es stellt sich die grundsätzliche Frage, wie man bei der Datenanalyse vorgehen soll, wenn man nicht weiss, wonach man sucht. D.h. man analysiert die Daten nicht mehr gezielt hypothesenbasiert oder aufgrund eines vorbestehenden Bauchgefühls, sondern rein auf der Basis dessen, was die Daten selbst hergeben. Hierzu braucht es künstliche Intelligenz, d.h. lernfähige Algorithmen. Bei der Bilderkennung hat man beispielsweise Analysetools darauf trainiert, Fotos richtig zu interpretieren, indem man ihnen schrittweise neue Elemente beigebracht und anschliessend ihre Performance getestet hat. Die grosse Schwierigkeit besteht nun darin, einem Computersystem beizubringen, Daten richtig zu interpretieren und selbst die richtigen Schlüsse daraus zu ziehen. Im Falle von autonomen Fahrzeugen kommen solche Cognitive-Computing-Ansätze zur Anwendung: Die Bandbreite an möglichen Situationen, mit denen ein Autolenker konfrontiert sein kann, ist so gross, dass man sie nicht alle im Voraus im System erfassen kann, sondern es braucht ein System, das selber lernfähig ist und auch in neuartigen Situationen die richtigen Entscheidungen trifft.
- **Standard-Werkzeuge für den Einsatz von Big Data:** Damit die Big Data-Technologie auch für KMUs erschwinglich wird, braucht es Standard-Werkzeuge mit entsprechenden Preismodellen. Die Werkzeuge müssen sich, ähnlich wie dies heute im Bereich des Data-Warehousing der Fall ist, mit den bestehenden Systemen über entsprechende Schnittstellen gut integrieren lassen. Heute stellt das Nicht-Vorhandensein solcher Standardwerkzeuge mit Blick auf die Nutzung von Big-Data-Technologie speziell für kleinere Unternehmen eine grosse Hürde dar. Es dürfte aber nur noch eine Frage der Zeit sein, bis solche Standardtools vorliegen werden; nach Einschätzungen eines der befragten Experten dürfte es in 3-5 Jahren soweit sein.
- **Beherrschung der Algorithmen:** Es besteht die Gefahr von Kontrollverlust aufgrund von Algorithmen, die man nicht mehr richtig versteht. Eine mögliche Vorsichtsmassnahme bestünde darin, von den Akteuren, welche Big-Data-Technologien einsetzen, einzufordern, dass sie die Algorithmen offenlegen, sodass sie für Fachleute allgemein nachvollziehbar sind.

## 5.7 Vier Horrorszenarien

Was die weitere Entwicklung im Bereich Big Data betrifft, wurden die Interview-Partner auch nach ihren Horrorszenarien und Idealvorstellungen befragt. Diese geben einen guten Anhaltspunkt, worauf die Data Governance auf gesellschaftlicher Ebene auszurichten ist bzw. welche Gefahren unbedingt vermieden werden sollten.

Grundsätzlich lassen sich vier Horrorszenarien unterscheiden, die unter Umständen auch in Kombination auftreten können:

Gemäss dem ersten Horrorszenario führt Big Data zu einer Zweiteilung der Welt: Ein paar wenige Daten-Monopole stehen einer grossen Zahl von Daten-Habenichtsen gegenüber. Die Daten-Monopole kommen zustande, indem in bestimmten Bereichen Daten und Informationen von einer Institution, Organisation oder Nation angeeignet, den übrigen vorenthalten, für eigene Zwecke ausgebeutet und gegebenenfalls manipuliert werden. Die daraus resultierenden sozialen Ungleichheiten und Ausbeutungsverhältnisse münden in sozialen Verwerfungen.

Gemäss dem zweiten Horrorszenario kann Big Data die Diskriminierung von Menschengruppen durch autoritäre Regime erleichtern. Ein autoritäres Regime, welches sich der Big-Data-Technologie bedient, wäre der gesellschaftliche Super-GAU. Die Enthüllungen von Edward Snowden zu den Überwachungstätigkeiten der NSA geben einen Vorgeschmack darauf, was in diesem Bereich alles möglich ist.

Gemäss dem dritten Horrorszenario führt die ständige Überwachung zu einer immer stärkeren Selbstzensur im Verhalten der Menschen und zur Unterdrückung jeglicher Kreativität. Damit laufen wir Gefahr, uns in eine Überwachungsgesellschaft zu verwandeln: es entsteht eine saubere, sterile Gesellschaft mit ganz vielen braven und passiven Konsumenten aber bar jeglicher Kreativität. Ob die Überwachung jedes Einzelnen auch tatsächlich stattfindet, ist dabei unerheblich. Nur schon das Wissen, dass potentiell jede Handlung überwacht wird und eine Auswirkung auf das zukünftige Leben haben kann, reicht für den psychologischen Effekt aus. Besonders kritisch an dieser Entwicklung ist, dass die Unterdrückung der Kreativität dazu führt, dass die Gesellschaft immer weniger dazu in der Lage ist, sich den Herausforderungen unserer Zeit zu stellen und tragfähige Lösungen zu entwickeln. Daher steigt auch die objektive Gefahr eines Teufelskreises, wenn als Antwort auf das erhöhte Schutzbedürfnis die Überwachung intensiviert wird.

Und gemäss dem vierten Horrorszenario läuft die Menschheit Gefahr, die Kontrolle über die Systeme zu verlieren: Die Eigendynamik der Systeme führt zu Kontrollverlust. Aufgrund der breitangelegten Datensammlung weiss das System bzw. die andere Seite mehr über uns als wir selber. Dabei sind wir vor Falschinterpretationen von Einzeldaten durch das System nicht gefeit, was aufgrund der zunehmenden Bedeutung von Daten in unserem Alltag verheerende Auswirkungen hat.

## **5.8 Vorstellungen einer idealen Big-Data-Welt**

Als Gegenentwurf zu den Horrorszenarien kann die ideale Big-Data-Welt dienen: Hier behalten die Menschen die Herrschaft über die eigenen personenbezogenen Daten und hinterlegen diese in einem Daten-Tresor bei einer Daten-„Bank“. Die Personendaten sind durch technische Vorkehrungen gesichert, und es ist nachvollziehbar, wer darauf zugegriffen hat. Dadurch lässt sich das Missbrauchspotential deutlich eindämmen.

Zudem gäbe es einen weltweiten Data-Space, in dem ein Maximum von nicht-personenbezogenen Daten aus dem öffentlichen Bereich und ein Maximum an Personendaten unter Kontrolle der Betroffenen zur allgemeinen Verwendung bereitgestellt werden. Dadurch würde sichergestellt, dass die zahlreichen Chancen, welche Big Data für Wirtschaft und Gesellschaft bietet, in der Praxis auch tatsächlich wahrgenommen werden.

Im Vergleich zur Funktionsweise heutiger Datenmonopoldienste, wie Amazon, Facebook, Apple oder Google, würde die Datenbesitzlage umgekehrt, ohne dass die Funktionalität dadurch reduziert würde: Dank virtueller Agenten und intelligenter Schnittstellen würden personalisierte Angebote weiterhin ermöglicht, ohne dass aber alle Profildaten durch einen Akteur zentral kontrolliert würden.

Auf der Ebene einzelner Unternehmen stünden in der idealen Big-Data-Welt alle Unternehmensdaten als Teil eines „Data Lakes“ zur Verfügung; die heutigen Silostrukturen wären damit aufgebrochen. Dank der Analyse der Daten würden Geschäftsprozesse effizienter und effektiver gestaltet und es könnten neue Geschäftsfelder erschlossen werden.

## **5.9 Wie können Organisationen dazu gebracht werden, Big Data regelkonform und sozial verträglich umzusetzen?**

Um zu erörtern, mit welchen Mitteln eine zweckmässige Governance im Big-Data-Bereich sichergestellt werden kann, wurden die befragten Experten danach gefragt, wie Organisationen dazu gebracht werden können, Big Data regelkonform und sozial verträglich umzusetzen. Hier lassen sich zwei Ebenen unterscheiden: die Sicht der einzelnen Organisation und die gesamtgesellschaftliche Sicht.

Aus der Perspektive der einzelnen Organisationen gibt es eine Reihe von Massnahmen und Vorkehrungen, die getroffen werden können, um sicherzustellen, dass die Nutzung der Daten im Rahmen der gesetzlichen Vorschriften und gemäss den ethischen Standards der jeweiligen Organisation erfolgt. Bei den befragten Unternehmen werden aktuell folgende Ansätze verfolgt:

- **Einhaltung der gesetzlichen, vertraglichen und internen Datenschutzbestimmungen**
- **Einhaltung von externen oder internen Codes of Conduct** o.ä. (mit Vorgaben zu Datenschutz, Qualität und ethischen Fragen)
- **Sensibilisierung der Mitarbeitenden** für die Belange des Datenschutzes
- **Technische oder organisatorische Massnahmen für den Schutz der Daten** (z.B. zweck- und rollengebundene Zugangsberechtigungen; Strikte Trennung von Identifikationsdaten und den übrigen Daten; Anwendung des Vier-Augen-Prinzips beim Zugang zu sensiblen Daten; Zugriffslogs; physische / technische Schranken)
- **Anonymisierung / Pseudonymisierung beim Daten-Import**
- **Verzicht auf den Bezug / die Weitergabe von personenbezogenen Daten**
- **Verzicht auf die Haltung heikler Daten** (z.B. Kreditkartendaten)
- **Verwendung von einfachen, kurzen und klaren Nutzungsbedingungen**, um für die Kunden Transparenz über die Verwendung der Daten herzustellen
- **Vertragliche Vereinbarungen mit hohen Konventionalstrafen** bei der Weitergabe von Daten an Dritte
- **Kontrollmechanismen:** interne und externe Kontrolle (Audits, Peer-Reviews, interne Ethikboards, denen alle Big-Data-bezogenen Projekte vorgelegt werden müssen, u.ä.)

Aus gesamtgesellschaftlicher Perspektive wurden folgende Massnahmen angeführt, um Organisationen dazu zu bringen, Big-Data-Technologien regelkonform und sozial verträglich anzuwenden:

- **Kontrollfunktion der Medien in Kombination mit einer kritischen Öffentlichkeit:** Investigativer Journalismus führt dazu, dass seitens der Öffentlichkeit Druck aufgebaut wird, wenn sich Unternehmen unethisch verhalten. Die kritische Diskussion von datenbezogenen Themen in den Medien führt zudem zu einer Sensibilisierung der betroffenen Unternehmen. Damit dieser Regulationsmechanismus über die Medien und eine kritische Öffentlichkeit funktioniert, müssen die Unternehmen sich im Klaren darüber sein, dass sie bei einem Leck oder einem Skandal ein echtes Problem haben.
- **Ethikkodizes / Labels:** Peer-Pressure sorgt dafür, dass Ethikkodizes etabliert werden. Gütesiegel auf der Basis von Zertifizierungen/Akkreditierungen erlauben eine Regulierung über den Markt (Image-Pflege).
- **In einzelnen Branchen spielt der Wettbewerb:** Die beiden vorgenannten Regulationsmechanismen funktionieren dann, wenn Unternehmen bei Datenschutz-Verstössen Imageschäden und Umsatzverluste befürchten müssen. Das setzt aber voraus, dass der Wettbewerb spielt. Gemäss Aussagen verschiedener Befragter ist dies vor allem in jenen Bereichen der Fall, wo in der Schweiz ein Markt für tangible Güter besteht, die einfach substituiert werden können. Auf internationalen Märkten und bei Netzwerkeffekten, die zur Bildung von Quasi-Monopolen führen, spielt der Wettbewerb jedoch oftmals nicht in der gewünschten Weise.
- **Staatliche Regulierung:** Gesetze und Vorschriften legen fest, was erlaubt und was nicht erlaubt ist. Bei Übertretungen können Bussen ausgesprochen werden. In schweren Fällen kann strafrechtlich gegen die Verantwortlichen vorgegangen werden.
- **Unabhängige Aufsichtsstelle:** Eine unabhängige Aufsichtsstelle nach dem Modell der Finanzmarktaufsicht übt die Aufsicht über die Datennutzer aus und stellt sicher, dass über die tatsächliche Verwendung der Daten Transparenz herrscht.

- **Globale Standards:** Angesichts der Tatsache, dass ein guter Teil der Unternehmen, die ganz massiv Personendaten sammeln und verwerten, auf internationaler Ebene operiert und nur bedingt dem schweizerischen Recht unterstellt ist, werden verschiedentlich auch globale Standards gefordert. Diese sind auch notwendig, um in Bereichen, wo der internationale Wettbewerb spielt, sicherzustellen, dass alle Unternehmen mit gleich langen Spiesen kämpfen.
- **Empowerment der Kunden und Nutzer:** Die Kunden bzw. die Nutzer müssen eine echte Wahl haben, welche personenbezogenen Daten sie zu welchem Zweck preisgeben. Dies setzt nicht nur eine entsprechende Sensibilisierung sondern auch eine Verbesserung der Human-Data-Interfaces voraus. Zudem muss zwischen den betroffenen Unternehmen der Markt spielen, oder es bedarf wirksamer Regulierungsmassnahmen. Möglicherweise ist auch der Einsatz von Intermediären nötig, welche es den Nutzern erleichtern, die Kontrolle über die Verwendung ihrer Daten auszuüben. Dabei sollte sich die Kontrolle der Nutzer auch auf neue Verwendungszwecke von bereits für andere Zwecke freigegebenen Daten erstrecken. In diesem Zusammenhang ist auch die Umsetzung des Rechts auf Vergessen zu diskutieren, das allerdings – wie einige der Befragten bemerkten – nicht absolut sein kann, da an gewissen personenbezogenen Daten ein öffentliches Interesse besteht, bzw. diese für das gute Funktionieren gewisser Dienste unerlässlich sind; man denke beispielsweise an einen Online-Marktplatz, bei dem Informationen über vergangene Transaktionen ausschlaggebend für den Aufbau von Reputation sind.
- **Data-Life-Cycle-Management:** Es werden technische Vorkehrungen getroffen, um Daten mit einer begrenzten Lebensdauer zu versehen. Dadurch reduziert sich das Missbrauchspotential, denn heute besteht die Schwierigkeit, einzelne Daten wieder aus den Datenbanken herauszukriegen. Die Idee wäre, dass man Daten bei der Erfassung mit einem Verfalldatum versieht; sie würden dann nach Ablauf der Frist automatisch gelöscht. Voraussetzung wäre, dass man zwischen unterschiedlichen Datentypen differenziert und dass ein Empowerment der Nutzer bei der Datenerfassung erfolgt.

Mehrere Befragte wiesen allerdings darauf hin, dass die Situation bereits ausser Kontrolle geraten sei und sich der Einsatz von Big Data nicht mehr regulieren lasse. Begründet wird dies einerseits damit, dass eine Regulierung auf internationaler Ebene kaum zustande kommen dürfte, obwohl eine solche dringend notwendig sei, um die Aktivität der international tätigen Grossunternehmen zu regulieren. Andererseits sei die Schweiz nur beschränkt souverän, wenn es darum geht, gegen Missbräuche von im Ausland domizilierten Grossfirmen oder ausländischen Nachrichtendiensten vorzugehen. Einzelne Befragte gaben auch zu bedenken, dass der Staat in Sachen Datenschutz nur beschränkt glaubwürdig sei, da er selber immer mehr personenbezogene Daten sammle. Von anderen Befragten wurde dem schweizerischen Datenschutz jedoch attestiert, dass er gegenüber den Schweizer Behörden recht gut funktioniere, aber hinsichtlich der privaten Akteure ohne Biss sei, während die Selbstregulierung durch die Unternehmen nicht oder nur teilweise funktioniere.

## 6 Sieben Thesen hinsichtlich einer „Good Data Governance“

Ausgehend von den Ergebnissen der Befragungen können im Hinblick auf eine „Good Data Governance“ sieben Thesen formuliert werden, welche die unterschiedlichen Perspektiven der befragten Experten auf die „Big Data“-Thematik in kondensierter Form wiedergeben, und welche anschliessend im Rahmen der quantitativen Befragung noch besser ausgeleuchtet und mit Zahlen unterlegt werden (siehe Kapitel 7).

<b>These 1</b>	<p><b>Beim Datenschutz braucht es einen Paradigmenwechsel.</b></p> <p>Dass es einen Paradigmenwechsel braucht, ist weitgehend unbestritten. Wie dieser aus- schauen soll ist noch unklar. Aufgrund der geführten Gespräche lassen sich folgende Tendenzen ausmachen:</p> <p><b>Empowerment der Nutzer:</b> Die Preisgabe und Nutzung von personenbezogenen Daten muss durch die betroffenen Personen effektiv kontrolliert werden können.</p> <p><b>Recht auf Anonymität:</b> Elementare Transaktionen des Lebens müssen auch anonym abgewickelt werden können.</p> <p><b>Technische Massnahmen:</b> Der Datenschutz ist insbesondere auch durch technische Massnahmen sicherzustellen.</p> <p><b>Wettbewerbsrechtlicher Ansatz:</b> Wenn wir einen besseren Schutz der Privatsphäre erreichen wollen, reicht es nicht, beim Datenschutz anzusetzen, sondern es braucht auch Massnahmen im Bereich der Wettbewerbsaufsicht.</p> <p>Des Weiteren ist angesichts der Entwicklungen im Big-Data-Bereich die Frage des Datenschutzes insbesondere auch mit Blick auf die vermehrte Zusammenführung von Daten aus ganz unterschiedlichen Quellen und die damit verbundene Möglichkeit der De-Anonymisierung von Personendaten neu zu beurteilen.</p>
<b>These 2</b>	<p><b>Der gesellschaftliche Nutzen von Daten erhöht sich, wenn sie als freie Infrastruktur-Ressourcen verfügbar sind.</b></p> <p>Dies gilt sowohl für nicht-personenbezogene Daten als auch für personenbezogene Daten.</p> <p><b>Open-Data-Prinzip:</b> Bei den nicht-personenbezogenen Daten führt die konsequente Anwendung des Open-Data-Prinzips zum grössten gesellschaftlichen Nutzen. Nicht-personenbezogene Daten sollen grundsätzlich zur freien Weiterverwendung zur Verfügung stehen. Ausnahmen sind Geschäftsgeheimnisse, sicherheitsrelevante Daten und urheberrechtlich geschützte Daten.</p> <p><b>Offene Personendaten:</b> Personenbezogene Daten sollen von den Betroffenen – je nach persönlichem Gutdünken – zur Weiterverwendung durch Dritte freigegeben werden. Hier ist ein Empowerment der Nutzerinnen und Nutzer vonnöten, so dass diese über ihre Personendaten verfügen und sie in Kenntnis des Verwendungszwecks gezielt für die Weiterverwendung freigeben können. Entsprechende Plattformen, welche die Freigabe und das Pooling von personenbezogenen Daten erleichtern, sind aus den USA und Grossbritannien im Rahmen der „My Data“-Initiative bereits bekannt<sup>3</sup>. Hier ist es</p>

<sup>3</sup> Das wohl bekannteste Beispiel ist das US-amerikanische „Blue Button“-Programm, das damit begann, dass Gesundheitsdienstleister für Armee-Veteranen den Patienten den Download der persönlichen Gesundheitsdaten ermöglichte, nachdem es eine gewisse Zahl diesbezüglicher Anfragen gegeben hatte. Mittlerweile wurde das Programm auf weitere Anbieter im Gesundheitsbereich ausgeweitet, und ähnliche Initiativen wurden für Energiedaten (Green Button) und Bildungsdaten (Red Button) als Teil einer breiter angelegten „My Data“-Initiative ins Leben gerufen.

	<p>wichtig, dass beispielsweise Bankdaten oder Gesundheitsdaten von den jeweiligen Dienstleistern in einem standardisierten Datenbezugsformat bereitgestellt werden, so dass sie von den Daten-Eignern (d.h. den Nutzerinnen und Nutzern) einfach gepoolt werden können, damit darauf aufbauend neuartige Dienstleistungen erbracht werden können. Denkbar sind beispielsweise Vergleichsdienste, Dienste zur Verhaltensbeeinflussung (z.B. Energieverbrauch, Bewegung, usw.) sowie personalisierte Angebote jeglicher Art. Darüber hinaus können die personenbezogenen Daten für Forschungszwecke freigegeben werden (z.B. für die medizinische Forschung).</p>
<b>These 3</b>	<p><b>Big Data verschärft eine Reihe von Gefahren, die abgewehrt werden müssen.</b></p> <p>Durch Big Data erhöht sich nicht nur die Wahrscheinlichkeit einer missbräuchlichen oder unerwünschten Nutzung oder Verknüpfung von Daten, sondern auch das damit verbundene Schadenspotential. Grundsätzlich lassen sich vier Arten von Gefahren unterscheiden: <b>staatliche Repression</b>, <b>ökonomische Diskriminierung</b>, <b>persönliche Repression</b> (diese lässt sich unter Umständen durch staatliche Repression oder ökonomische Diskriminierung institutionalisieren) sowie die <b>unkontrollierte Eigen-dynamik der Systeme</b> (Gefahr von Algorithmen, die man nicht mehr richtig versteht und beherrscht).</p>
<b>These 4</b>	<p><b>Machtgefälle aufgrund von einseitiger Datenkontrolle gilt es zu vermeiden.</b></p> <p>Mittel zur Reduktion von Machtgefällen sind die Umsetzung des <b>Transparenz-Prinzips</b> (alle Daten von politischer Relevanz müssen offen zugänglich sein), die <b>Kontrolle bzw. die Zerschlagung von Monopolen/Oligopolen</b> sowie der <b>Schutz vor staatlichem Missbrauch von Personendaten</b>. Hinsichtlich des letzten Punktes ist es nach Aussagen von Befragten wichtig, dass der Kampf gegen den Terrorismus oder andere Misstände nicht als Vorwand dienen, um die Schutzmechanismen gegen staatlichen Missbrauch von Personendaten abzubauen.</p>
<b>These 5</b>	<p><b>Es sollte ein liberaler Ansatz verfolgt werden.</b></p> <p>Dieser kennzeichnet sich durch die konsequente Anwendung des <b>Marktprinzips</b> und eine <b>Befähigung der Nutzer</b>. Ein liberaler Ansatz basiert auf den Prämissen, dass sich Datenschutz und Data-Sharing über Marktmechanismen regulieren lassen und dass Nutzerinnen und Nutzer mittels geeigneter Software-Lösungen, Transparenz-Auflagen für Unternehmen sowie Aufklärungs- und Bildungsmaßnahmen dazu gebracht werden können, einen bewussten und informierten Umgang mit ihren Daten zu pflegen.</p>
<b>These 6</b>	<p><b>Staatliche Intervention ist nötig.</b></p> <p>Die Notwendigkeit von staatlichen Interventionen ergibt sich aus dem <b>Marktversagen</b> und der <b>Überforderung der Nutzer</b>. In etlichen Bereichen ist zu beobachten, dass der Daten-Markt aufgrund von natürlichen Monopolen, Informations-Asymmetrien und negativen Externalitäten versagt. Zudem sind Kunden bzw. Nutzer nicht in der Lage, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen.</p>
<b>These 7</b>	<p><b>Data Governance muss im internationalen Kontext angegangen werden.</b></p> <p>Die Hauptgefahr in Sachen Datenschutz geht von <b>multinationalen Grossfirmen</b> aus, gegen die einzelne Staaten nicht viel ausrichten können. Zudem führen einzelstaatliche Lösungen auf internationalen Märkten zu <b>Wettbewerbsverzerrungen</b> und im Endeffekt zu einer Verwässerung der Standards. Die Situation verschärft sich dadurch, dass digitalen Daten heute kein geographischer Ort mehr zukommt, da sie weltweit verteilt sind.</p>

Tabelle 6: Sieben Thesen hinsichtlich einer „Good“ Data Governance

## 7 Ergebnisse der quantitativen Erhebung

### 7.1 Repräsentativität der Ergebnisse

Es bestand bei der Datenerhebung grundsätzlich kein Anspruch darauf, dass die Befragung für die Schweizer Bevölkerung als Ganze repräsentativ ist. Vielmehr richtete sie sich an die Menschen in der Schweiz, die sich in irgendeiner Form mit Big Data auseinandersetzen. Da die Gesamtheit und Zusammensetzung dieser Zielgruppe nicht bekannt ist, wurde darauf geachtet, dass Personen aus möglichst unterschiedlichen Bereichen und mit unterschiedlichen Sensibilitäten in die Umfrage einbezogen wurden (Anhang 4 gibt Aufschluss über die Kategorisierung der Teilnehmenden, die vor der Kontaktnahme vorgenommen wurde, die Anzahl Personen pro Kategorie sowie die entsprechende Rücklaufquote). Dank dem Einbezug von Personen mit ganz unterschiedlichen Profilen, ist es möglich, die Ergebnisse der Befragung nach unterschiedlichen Stakeholder-Gruppen aufzuschlüsseln und aufzuzeigen, in welchen Fragen über alle Gruppen hinweg ein breiter Konsens herrscht bzw. zu welchen Fragen sich die Geister scheiden. Aufgrund dieser Analysen lässt sich zu einem gewissen Grad auch eruieren, in welchen Punkten eine repräsentative Umfrage zu anderen Ergebnissen gekommen wäre (siehe Kapitel 6.10).

821 Personen haben den Fragebogen komplett ausgefüllt, darunter 764 direkt Kontaktierte und 57 via den „Open Call“. Damit beläuft sich die Rücklaufquote bei den direkt Kontaktierten auf 27%, was ein gutes Ergebnis darstellt. Die Rücklaufquote der Männer beträgt 28% und jene der Frauen 26%; dieser Unterschied ist statistisch nicht signifikant<sup>4</sup>. Die französischsprachigen Adressaten haben sich bei einer Rücklaufquote von 35% häufiger an der Umfrage beteiligt als die deutschsprachigen (26%), was darauf zurückzuführen sein dürfte, dass der deutschsprachige Verteiler mehr Personen umfasste, die keinen direkten Bezug zur Big-Data-Thematik aufweisen, als der französischsprachige. Und schliesslich war die Rücklaufquote bei der persönlichen Kontaktnahme mit 28% deutlich höher als bei der Kontaktnahme via eine Organisation (9%).

Um ein besseres Verständnis zu erlangen, welche Personen sich an der Umfrage beteiligt haben, und welche eher nicht, haben wir zudem die Charakteristika der Personen, welche mit dem Ausfüllen des Fragebogens zwar begonnen, die Umfrage aber nicht beendet haben, mit jenen verglichen, welche den Fragebogen komplett ausgefüllt haben. Diese Analyse führte zu folgenden Ergebnissen:

Die Abschlussquote beträgt insgesamt rund 78%<sup>5</sup>. Erwartungsgemäss haben Personen, die beruflich oft mit Daten zu tun haben, eine deutlich höhere Abschlussquote als die übrigen (79% vs. 59%). Und unter jenen, die beruflich mit Daten zu tun haben, haben wiederum jene eine deutlich höhere Abschlussquote, in deren Unternehmen oder Organisation im Umgang mit Daten mindestens eines der drei „V“ von Big Data („Volume“, „Variety“, „Velocity“) eine wichtige Rolle spielt (84% vs. 54%). Ebenso weisen Personen, die sich im Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinandersetzen, eine deutlich höhere Abschlussquote auf (82% vs. 74%). Bei den wenigen Personen, welche angeben haben, dass sie überhaupt keinen Bezug zu Daten haben, beträgt die Abschlussquote nur knapp 50%. Interessanterweise hatte die Frage, ob sich jemand zivilgesellschaftlich oder politisch für datenbezogene Belange einsetzt, keinen Einfluss auf die Abschlussquote.

Während bei der Rücklaufquote kein Gender-Effekt zu beobachten ist, tendieren Männer, die damit angefangen haben, den Fragebogen auszufüllen, eher dazu, ihn auch fertig auszufüllen (Männer: 79%; Frauen: 70%). Dieser Effekt besteht auch unter jenen Personen, die oft beruflich mit Daten zu tun

<sup>4</sup> Im vorliegenden Bericht beziehen sich Angaben hinsichtlich der statistischen Signifikanz sofern nicht anders angegeben auf ein Signifikanzniveau von 0.05.

<sup>5</sup> Als „abgeschlossen“ wird die Umfrage dann betrachtet, wenn der Fragebogen bis zum Schluss ausgefüllt wurde und höchstens 3 von 13 obligatorischen Fragen ganz ausgelassen oder nur sehr lückenhaft ausgefüllt wurden. Als „abgebrochen“ wird die Umfrage dann betrachtet, wenn mindestens 5 von 13 obligatorischen Fragen beantwortet wurden, die Umfrage aber nicht „abgeschlossen“ wurde. Fälle, in denen höchstens 4 Fragen beantwortet wurden, werden bei der Analyse der Abschlussquoten nicht berücksichtigt.

haben. Betrachtet man jedoch das Tätigkeitsfeld „Technik, Informatik“ gesondert, so verschwindet der Gender-Effekt. Das könnte ein Hinweis darauf sein, dass wir es nicht mit einem echten Gender-Effekt zu tun haben, sondern dass dieser primär durch die ungleiche Geschlechterverteilung im beruflichen Tätigkeitsfeld „Technik, Informatik“ zu erklären ist.

Die Abschlussquote nimmt mit steigendem Alter zu und flacht bei 60 Jahren ab (unter 40 Jahre: 68%; 40-49 Jahre: 78%; 50-59 Jahre: 82%; 60 Jahre oder älter: 78%). Im Gegensatz zum Gender-Effekt, wird der Alterseffekt nicht neutralisiert, wenn man das berufliche Tätigkeitsfeld „Technik, Informatik“ gesondert betrachtet; im Gegenteil – er ist dort sogar noch ausgeprägter.

Umfrageteilnehmer, welche in kleinen Unternehmen bzw. Organisationen tätig sind, haben eine höhere Abschlussquote als jene, die für mittlere oder grosse Unternehmen bzw. Organisationen arbeiten (10-49 VZÄ: 87%; über 50 VZÄ: 77%). Dieser Grösseneffekt entfällt, wenn man das berufliche Tätigkeitsfeld „Technik, Informatik“ gesondert betrachtet.

Es konnten teilweise regionale Effekte bezüglich der Wohnregion der Umfrageteilnehmenden festgestellt werden. So weisen Personen, welche in der Region Nordwestschweiz wohnhaft sind, mit 85% eine höhere Abschlussquote auf als Personen, die in der Ostschweiz (70%), in der Genferseeregion (71%), im Raum Zürich (76%) oder im Kanton Bern (77%) wohnen. Interessanterweise wurden keine solchen Effekte bezüglich der Region festgestellt, in der die Befragten arbeiten.

Befragte, welche „Technik, Informatik“ als berufliches Tätigkeitsfeld angeben, in dem sie mit Daten zu tun haben, haben eine höhere Abschlussquote als die übrigen (81% vs. 74%). Besonders hoch ist die Abschlussquote unter jenen Personen, welche angeben, nicht nur in den Bereichen „Forschung, Entwicklung“ oder „Technik und Informatik“ mit Daten zu tun zu haben, sondern parallel dazu auch bei administrativen oder juristischen Tätigkeiten. Interessanterweise ist hier die Abschlussquote deutlich höher als bei den Befragten, welche nur das Tätigkeitsfeld „Technik, Informatik“ angegeben haben (84% vs. 76%). Dabei umfasst die Gruppe der Personen, welche Tätigkeiten im Bereich „Technik, Informatik“ mit administrativen oder juristischen Tätigkeiten kombinieren, vergleichsweise viele ältere Menschen in grösseren Unternehmen oder Organisationen (mehr als ein Viertel ist über 50 und in einem Grossunternehmen bzw. einer grossen Organisation mit über 250 VZÄ tätig). Dies könnte den oben beschriebenen Alterseffekt, der bei den Befragten im Tätigkeitsfeld „Technik, Informatik“ besonders ausgeprägt ist, erklären.

Erwartungsgemäss hat die Sprache der Umfrageteilnehmer keinen Einfluss auf die Abschlussquote. Der Unterschied bei der Rücklaufquote zwischen Deutsch- und Westschweizern erklärt sich daher allein durch die unterschiedliche Methode beim Zusammenstellen der Kontaktdaten. Auch hat es keinen Einfluss auf die Abschlussquote, ob jemand im öffentlichen oder im privaten Sektor tätig ist. Ebenso wenig konnte ein Zusammenhang mit dem thematischen Fokus des zivilgesellschaftlichen oder politischen Engagements der Befragten festgestellt werden.

Als Fazit können wir daher festhalten, dass die unterschiedlichen Abschlussquoten weitestgehend der Intention entsprechen, die mit dem Fragebogen verfolgt wurde: Personen, welche beruflich mit Aspekten von Big Data zu tun haben oder sich persönlich mit der Thematik auseinandersetzen, waren eher geneigt, den Fragebogen auszufüllen. Dafür spricht auch, dass offenbar ältere Menschen mit einem breiteren Erfahrungshorizont besonders geneigt waren, den Fragebogen bis zum Ende auszufüllen.

Die beobachteten Verzerrungen hinsichtlich Geschlecht und Alter der Befragten sowie bezüglich der Unternehmensgrösse lassen sich durch die Struktur der Zielgruppe erklären: Frauen sind in den entsprechenden Berufsgruppen stark untervertreten, während die Gruppe der Menschen, welche Tätigkeiten in den Bereichen „Technik, Informatik“ oder „Forschung, Entwicklung“ mit administrativen und juristischen Tätigkeiten verbinden zu einem Grossteil aus Männern über 50 besteht. Die Befragung dürfte demnach hinsichtlich der intendierten Zielgruppe weitgehend repräsentativ sein.

Wie in Kapitel 7.10.4 näher ausgeführt, dürfte auch die Repräsentativität der Umfrage in Bezug auf die schweizerische Gesamtbevölkerung mit Ausnahme einiger kleinerer Verzerrungen gegeben sein.

## 7.2 Eigenschaften der befragten Personen (Beschreibung der Stichprobe)

### 7.2.1 Geschlecht, Alter, Sprache, Wohn- und Arbeitsort

Bei 84% der Befragten handelt es sich um Männer. Diese sehr einseitige Geschlechterverteilung widerspiegelt die ungleiche Geschlechterverteilung im Tätigkeitsfeld „Technik und Informatik“, in dem über zwei Drittel der Befragten aktiv sind.<sup>6</sup> Was das Alter betrifft, so sind die Hälfte der Befragten über 50 Jahre alt. Die 50 bis 59-Jährigen sind denn auch die am stärksten vertretene Altersgruppe (37% der Befragten), gefolgt von den 40 bis 49-Jährigen (32%). Dabei sind die Frauen tendenziell etwas jünger als die Männer: 53% der Männer bzw. 37% der Frauen sind 50 oder älter, während 31% der Frauen, aber nur 15% der Männer unter 40 sind (siehe Abbildung 1).

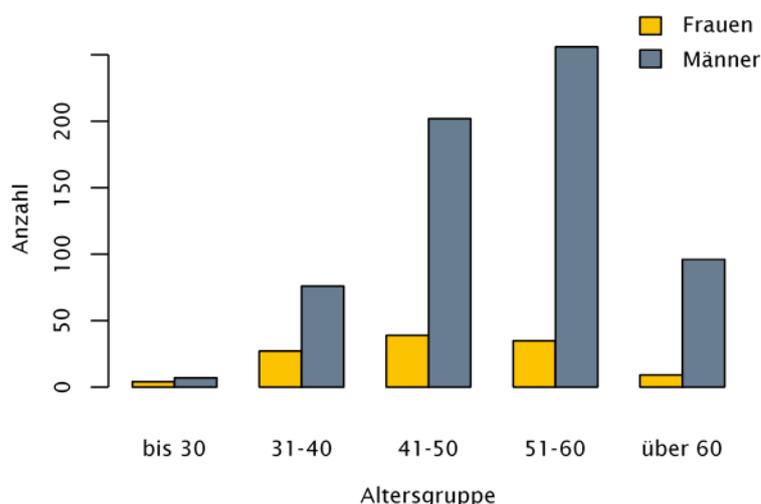


Abbildung 1: Altersverteilung nach Geschlecht

Was die Sprachverteilung anbelangt, stellen die Deutschsprachigen mit rund 81% der Befragten die grösste Gruppe dar, während die Französischsprachigen rund 18% und die Italienischsprachigen rund 1% der Stichprobe ausmachen. Letztere Zahl wurde aus der Sprachpräferenz der Personen hochgerechnet, welche am Ende des Fragebogens ihre Kontaktdaten angegeben hatten. Damit sind die Deutschsprachigen im Vergleich zur ständigen Schweizer Wohnbevölkerung etwas übervertreten (81% vs. 73%) und die Französischsprachigen etwas untervertreten (18% vs. 23%), während die Italienischsprachigen deutlich untervertreten sind (1% vs. 6%).

<sup>6</sup> Zum Vergleich die aktuellen Zahlen des Bundesamts für Statistik hinsichtlich der Geschlechterverteilung (Frauenanteil) bei den Personen, die sich in den Bereichen Technik und Informatik in Ausbildung befinden bzw. kürzlich ein Studium angetreten haben:

- Berufliche Grundbildung, Informatik: 6.1%
- Berufliche Grundbildung, Ingenieurwesen und Technik: 5.4%
- Eintritte in Fachhochschulen, Technik und IT: 10.1%
- Eintritte in universitäre Hochschulen, Technische Wissenschaften: 29.3%

Quellen: BFS, Lernende – Berufliche Grundbildung nach Bildungsfeldern und Geschlecht, 2013; BFS, SHIS – Eintritte in Fachhochschulen nach Fachbereichsgruppe, 2014; BFS, SHIS – Eintritte in universitäre Hochschulen nach Fachbereichsgruppe, 2014.

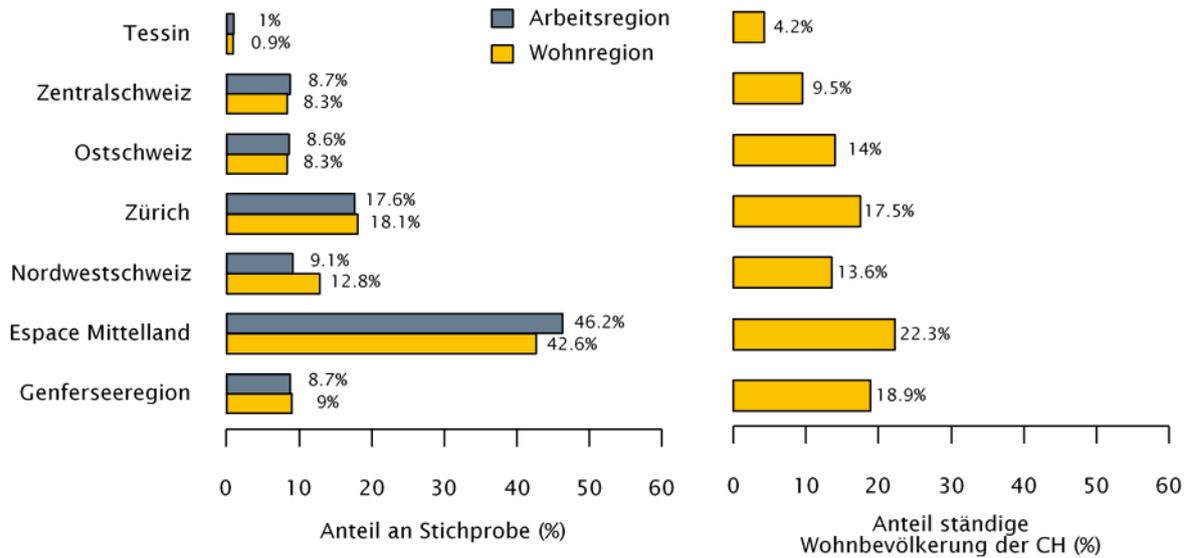


Abbildung 2 gibt einen Überblick über die geografische Verteilung der Befragten. Hier fällt auf, dass der Espace Mittelland in der Stichprobe stark übervertreten ist, während das Tessin, die Genferseeregion und die Ostschweiz stark untervertreten sind. Bei den Regionen Nordwestschweiz, Zürich und Zentralschweiz hingegen entsprechen die Werte in etwa jenen der Wohnbevölkerungsstatistik. Diese Übervertretung des Espace Mittelland und die Untervertretung der Regionen, die am weitesten von Bern entfernt sind, dürfte auf zwei Faktoren zurückzuführen sein: Einerseits wurden viele Personen aus der Bundesverwaltung zur Teilnahme an der Umfrage eingeladen. Diese tendieren dazu, im Espace Mittelland zu wohnen und zu arbeiten. Andererseits wurde beim Zusammenstellen des E-Mail-Verteilers teilweise auch auf das Kontaktnetz des in Bern ansässigen E-Government-Instituts zurückgegriffen. Auch hier dürften Personen aus dem Kanton Bern und den umliegenden Kantonen übervertreten sein.

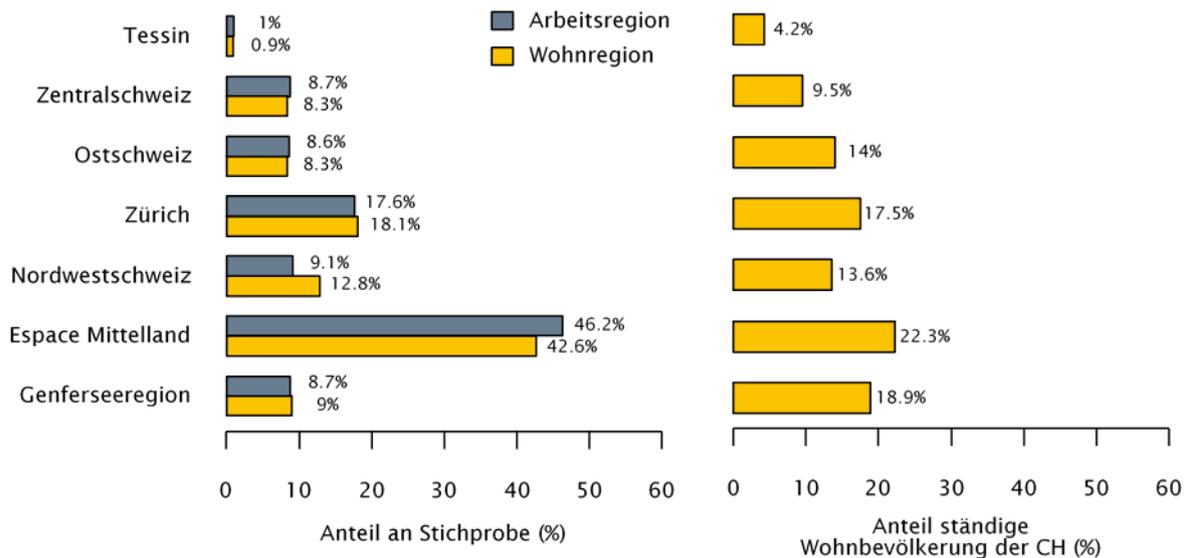


Abbildung 2: Verteilung nach Wohn- und Arbeitsregion im Vergleich mit der ständigen Wohnbevölkerung

## 7.2.2 Persönlicher Bezug zu Daten

Die Befragten wurden nach ihrem persönlichen Bezug zu Daten gefragt. Wie aus Abbildung 3 ersichtlich ist, haben praktisch alle Befragten (95%) oft beruflich mit Daten zu tun; 41% setzen sich in ihrem Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinander, während sich 36% im Rahmen einer politischen Tätigkeit oder eines zivilgesellschaftlichen Engagements für datenbezogene Belange einsetzen. Knapp 2% geben zusätzlich einen weiteren Bezug zu Daten an und verweisen dabei auf die persönliche Betroffenheit, ein persönliches Interesse oder einen ausserberuflichen Umgang mit Daten (Verein, Hobby, Studium, Kunst). Und schliesslich geben etwas weniger als 1% der Befragten an, keinen Bezug zu Daten zu haben. Dieser sehr niedrige Wert entspricht der Zielsetzung der Umfrage, welche sich an Menschen richtete, die einen persönlichen Bezug zu Daten haben.

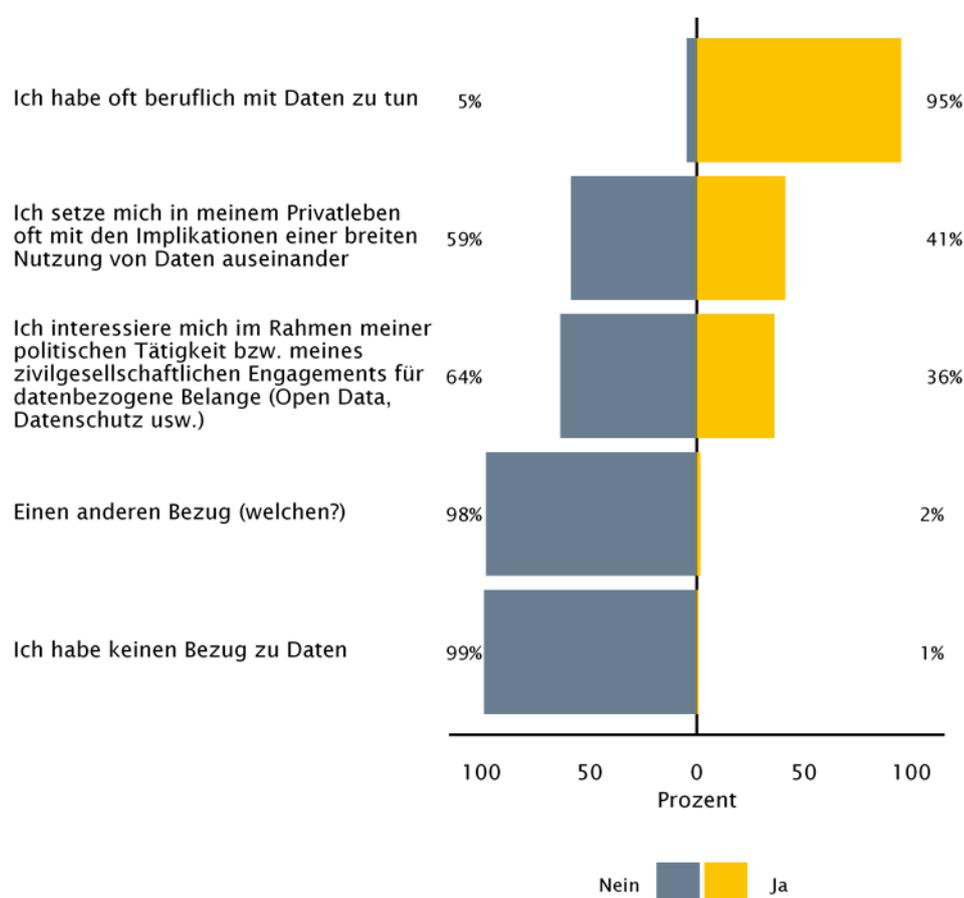


Abbildung 3: Persönlicher Bezug zu Daten

Jene Befragten, welche oft beruflich mit Daten zu tun haben, wurden nach ihren Tätigkeitsfeldern gefragt, in denen sie mit Daten zu tun haben. Abbildung 4 gibt einen Überblick, wie häufig die verschiedenen Tätigkeitsfelder genannt wurden: An erster Stelle figuriert „Technik, Informatik“ (68% gaben an, in diesem Tätigkeitsfeld mit Daten zu tun zu haben), gefolgt von „Unternehmensführung, Management“ (43%) und „Administrative Tätigkeit“ (40%). Je rund ein Viertel nannten „Marketing, Kommunikation“ (27%) bzw. „Forschung und Entwicklung“ (25%). Drei weitere Tätigkeitsfelder wurden von knapp einem Fünftel der Befragten genannt: „Juristische Tätigkeit“ (18%), „Personalwesen (17%)“ und „Unterricht, Lehre“ (16%). Am wenigsten Nennungen erhielten „Produktion“ (7%) und „Einkauf / Logistik“ (7%).

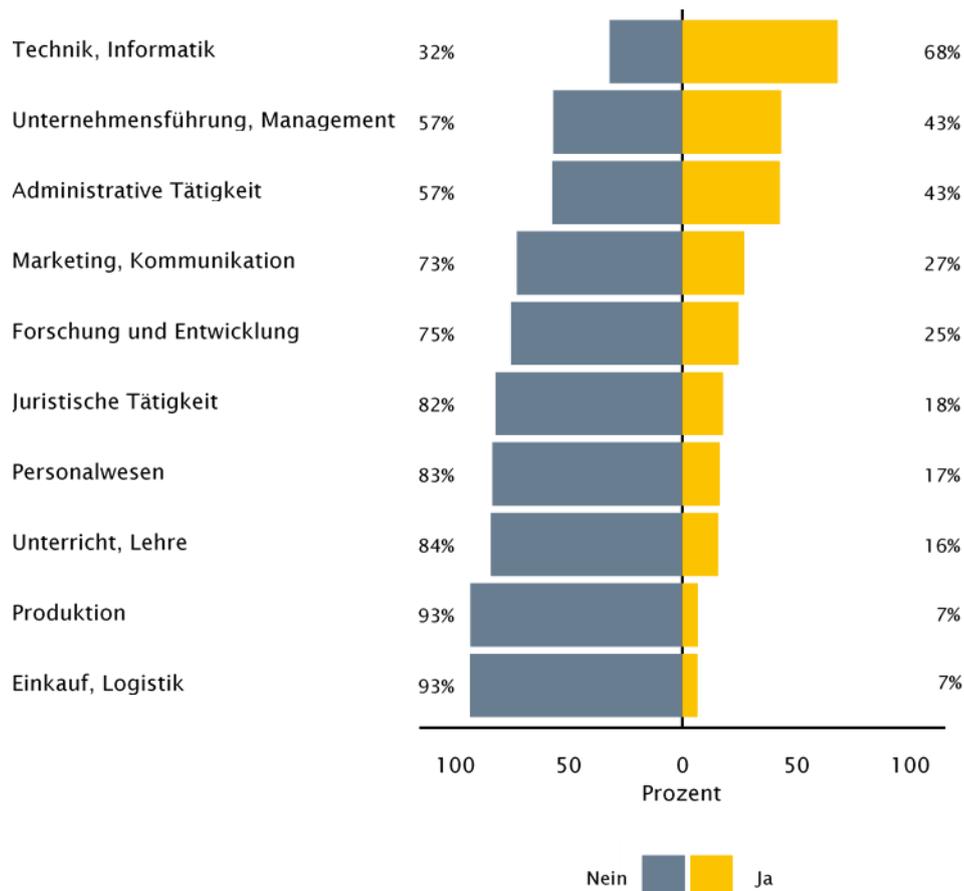


Abbildung 4: Tätigkeitsfelder der Personen, die oft beruflich mit Daten zu tun haben

Auf der Basis einer Analyse der Mehrfachnennungen wurden die Tätigkeitsfelder gruppiert (siehe Abbildung 5). Dabei erwies sich eine Abgrenzung der Tätigkeitsfelder „Technik, Informatik“, „Forschung, Entwicklung“ und der administrativen bzw. juristischen Tätigkeiten am ergiebigsten, da sie vergleichsweise wenig Überschneidungen aufweisen. In der Abbildung ist zudem ersichtlich, welcher Anteil der einzelnen Gruppen zusätzlich auch „Unternehmensführung, Management“ als Tätigkeitsfeld angibt. Hier zeigt sich, dass die Führungskräfte in der Gruppe der Befragten, welche „Technik, Informatik“ oder „Forschung, Entwicklung“ in Kombination mit juristischen oder administrativen Tätigkeiten angeben, am stärksten vertreten sind (insgesamt gehören 41% aller befragten Führungskräfte dieser Gruppe an).

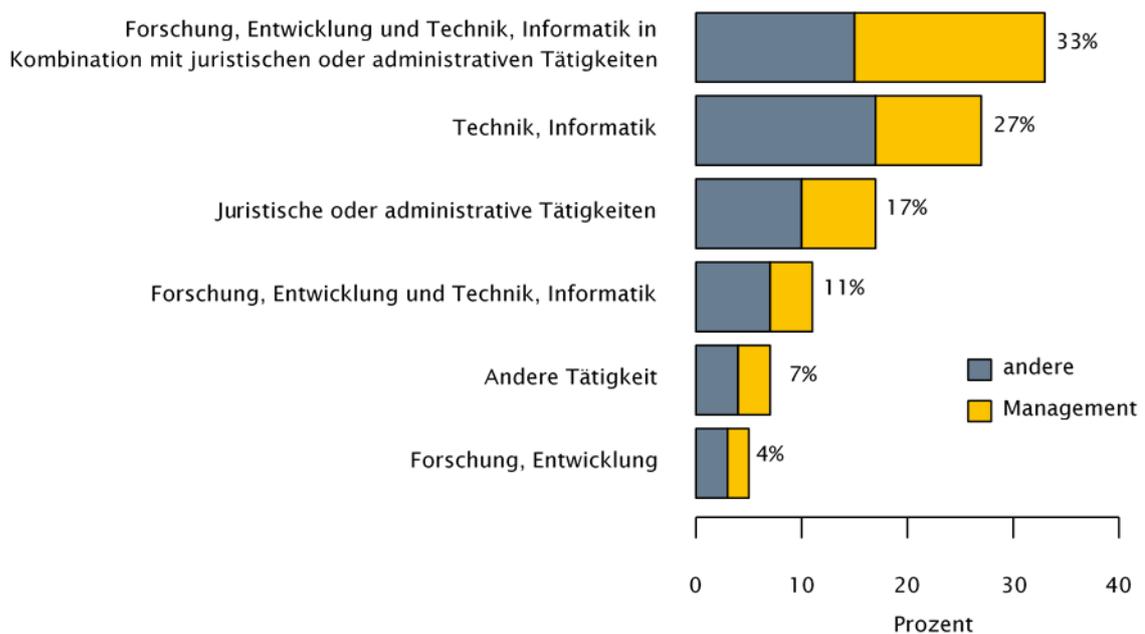


Abbildung 5: Tätigkeitsfelder der Personen, die oft beruflich mit Daten zu tun haben (gruppiert)

Abbildung 6 gibt einen Überblick über die Branchen (aufgeschlüsselt nach Sektoren), in denen jene Befragten, die oft beruflich mit Daten zu tun haben, nach eigenen Angaben tätig sind: Die grösste Gruppe bilden mit einem Anteil von 32% jene Befragten, die in der öffentlichen Verwaltung tätig sind und ihre Organisation der Branche „Management, Administration, Rechtswesen“ zuordnen. Die zweitgrösste Gruppe bilden mit einem Anteil von 16% die Befragten, die bei einem Privatunternehmen der Branche „Technik, Informatik, Ingenieurwesen“ tätig sind, gefolgt von den im öffentlichen Sektor im Bereich „Unterrichtswesen, Forschung, Medien, Kultur“ Beschäftigten (11%). Seitens der Privatwirtschaft sind zudem die Branchen „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (6%) und „Management, Administration, Rechtswesen“ (3%) mit nennenswerten Anteilen vertreten. Seitens der Mitarbeitenden des öffentlichen Sektors wurden die Branchen „Technik, Informatik, Ingenieurwesen“ (5%) und „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (5%) relativ oft genannt.

Die Umfrageteilnehmer wurden auch nach der Rechtsform und der Grösse ihres Unternehmens bzw. ihrer Organisation gefragt. Wie aus Abbildung 7 hervorgeht, arbeiten etwas über 60% der Befragten bei einer öffentlich-rechtlichen Organisation, 30% bei einem privatrechtlichen, gewinnorientierten Unternehmen und rund 5% bei einer privatrechtlichen, gemeinnützigen Organisation oder einer Mischform. Damit ist der öffentlich-rechtliche Sektor angesichts der Statistik der Unternehmensstruktur des BFS von 2013 stark übervertreten (64% vs. 13%), während die Privatwirtschaft stark untervertreten ist (30% vs. 84%). Bei den öffentlich-rechtlichen Organisationen handelt es sich mehrheitlich um grosse Organisationen mit mehr als 250 Mitarbeitenden (in Vollzeitäquivalenten). Dies entspricht der Grössenverteilung der Einheiten gemäss der amtlichen Statistik, wobei die kleineren Einheiten in unserer Stichprobe etwas übervertreten sind. Bei den privatwirtschaftlichen Unternehmen ist die Zusammensetzung durchmischert, wobei in unserer Stichprobe wiederum die Kleinstunternehmen (0 bis 9 Mitarbeitende) und die kleinen Unternehmen (10 bis 49 Mitarbeitende) gegenüber den mittleren und grossen Unternehmen etwas übervertreten sind.

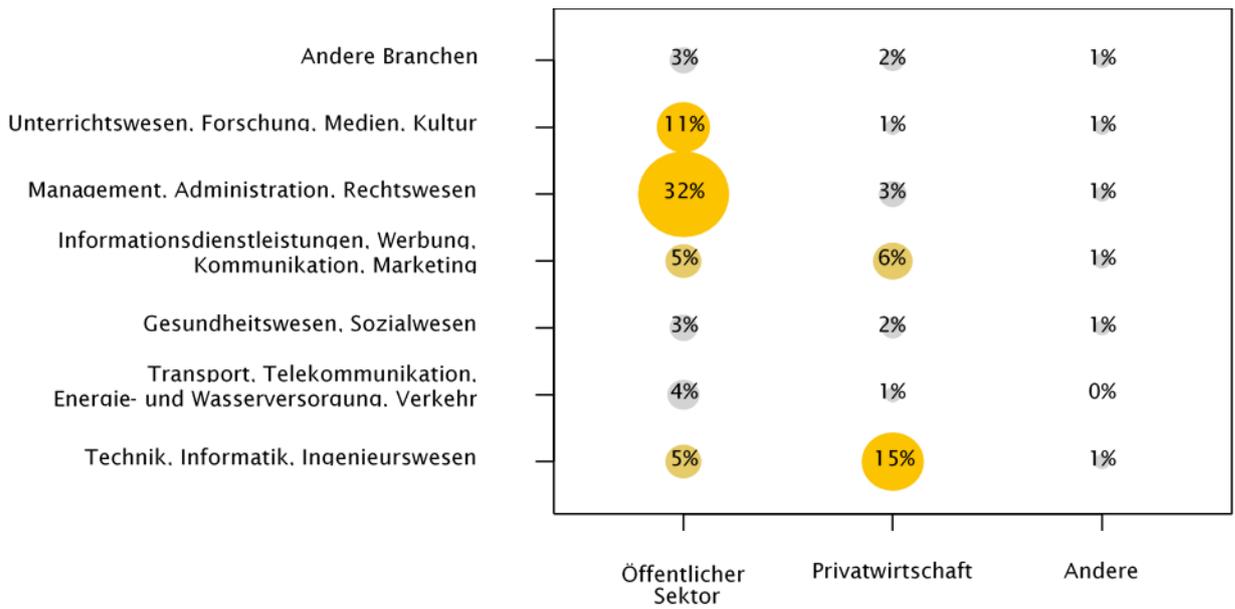


Abbildung 6: Branchen, in denen jene Personen tätig sind, die oft beruflich mit Daten zu tun haben (gruppiert, aufgeschlüsselt nach Sektoren)

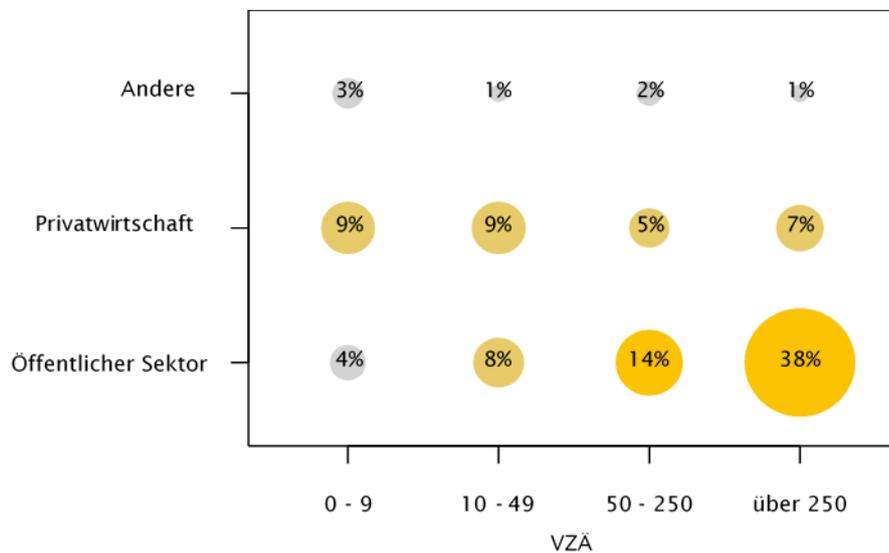


Abbildung 7: Rechtsform und Grösse der Unternehmen/Organisationen, denen jene Personen angehören, die oft beruflich mit Daten zu tun haben

Jene Befragten, welche angegeben hatten, dass sie sich im Rahmen ihres politischen oder zivilgesellschaftlichen Engagements für datenbezogene Belange interessieren, wurden nach den Aspekten gefragt, die im Rahmen ihres Engagement eine wichtige Rolle spielen. Die Ergebnisse können der Abbildung 8 entnommen werden: An erster Stelle fungieren mit je etwas über 80% Nennungen der Datenschutz und der freie Zugang zu Wissen, gefolgt vom Recht auf informationelle Selbstbestimmung (75%) und der freien Weiterverwendung von nicht-personenbezogenen Daten (72%). Über die Hälfte engagieren sich zudem auch für die Förderung von Medien-/IT- und Datenkompetenz (57%) und für die Innovationsförderung (55%). Etwas weniger häufig, aber immerhin noch von über einem Drittel der Befragten wurden die Weiterverwendung von personenbezogenen Daten (41%), der Konsumentenschutz (34%) und die Standortförderung (34%) genannt.

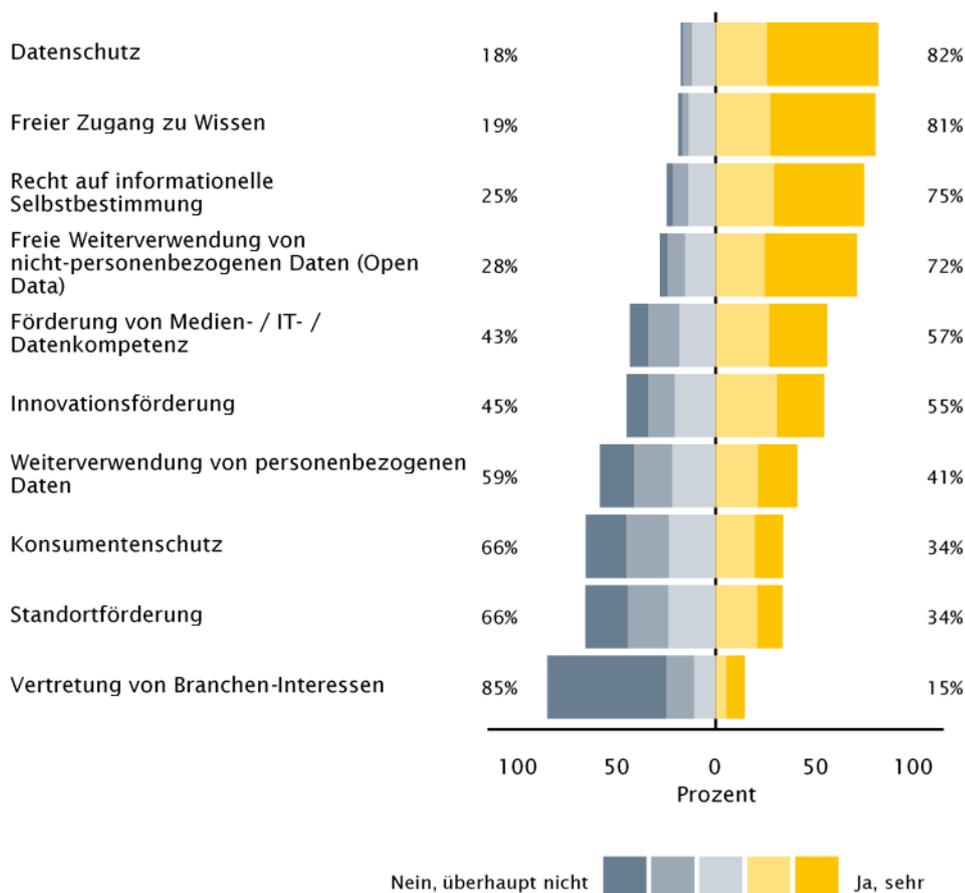


Abbildung 8: Datenbezogene Aspekte, welche im Rahmen des politischen oder zivilgesellschaftlichen Engagements eine Rolle spielen

Wenn man die genannten Aspekte des politischen und zivilgesellschaftlichen Engagements mithilfe einer Hauptkomponentenanalyse gruppiert, und die Antworten der Befragten daraufhin analysiert, auf welchen Bereich sie im Rahmen ihres zivilgesellschaftlichen bzw. politischen Engagements ihr Hauptaugenmerk legen, so zeichnet sich folgendes Bild (siehe Abbildung 9): Etwas über die Hälfte der Befragten, die angeben, dass sie sich im Rahmen ihrer politischen Tätigkeit bzw. ihres zivilgesellschaftlichen Engagements für datenbezogene Belange interessieren, legen ihren Hauptfokus auf Open Data bzw. freien Zugang zu Wissen. 13% legen ihren Hauptfokus auf Anliegen wie Datenschutz, Konsumentenschutz, Recht auf informationelle Selbstbestimmung bzw. Weiterverwendung von personenbezogenen Daten, während sich 4% hauptsächlich der Standort- oder Innovationsförderung, der Förderung von Medien-/IT-/Datenkompetenz bzw. der Vertretung von Branchen-Interessen widmen. Fast ein Drittel der Befragten gibt mehrere Schwerpunkte an, wobei insbesondere die Kombination von Anliegen im Bereich Open Data / freier Zugang zu Wissen mit Anliegen im Bereich des Daten- und Konsumentenschutzes im Vordergrund steht.

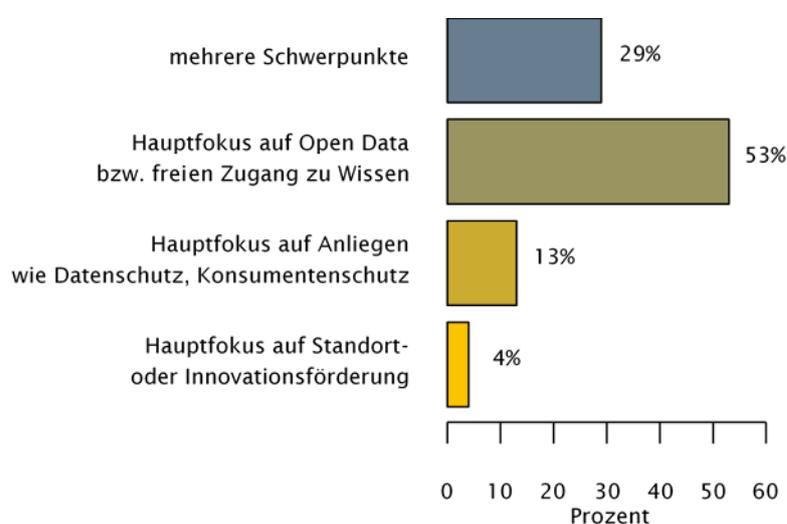


Abbildung 9: Hauptfokus des politischen oder zivilgesellschaftlichen Engagements im Bereich der Daten (gruppiert)

### 7.3 Datenbezogene Praktiken in Unternehmen/Organisationen

Die Befragten, welche oft beruflich mit Daten zu tun haben, wurden gebeten zu präzisieren, welche datenbezogenen Praktiken in ihrem Unternehmen eine wichtige Rolle spielen. Wie aus der Abbildung 10 hervorgeht, stehen die klassischen drei „V“ an erster Stelle: die Verarbeitung von grossen Datenmengen („Volume“), die rasche Verarbeitung von aktuellen Daten („Velocity“), sowie die Verknüpfung von heterogenen Datenbeständen aus unterschiedlichen Quellen („Variety“). Dabei geben 42% der Befragten an, dass alle drei Kern-Aspekte von Big Data in ihrem Unternehmen bzw. in ihrer Organisation eine wichtige Rolle spielen, bei 29% sind es zwei Kern-Aspekte, bei weiteren 18% ist es immerhin noch einer, während 10% der Befragten angeben, dass weder „Volume“, „Variety“, noch „Velocity“ in ihrem Unternehmen/ihrer Organisation eine wichtige Rolle spielen. Demnach scheint Big Data für rund zwei Fünftel der Befragten in ihrem beruflichen Kontext bereits Realität zu sein, während zusätzlich knapp die Hälfte zumindest mit bestimmten Aspekten davon vertraut sein dürfte.

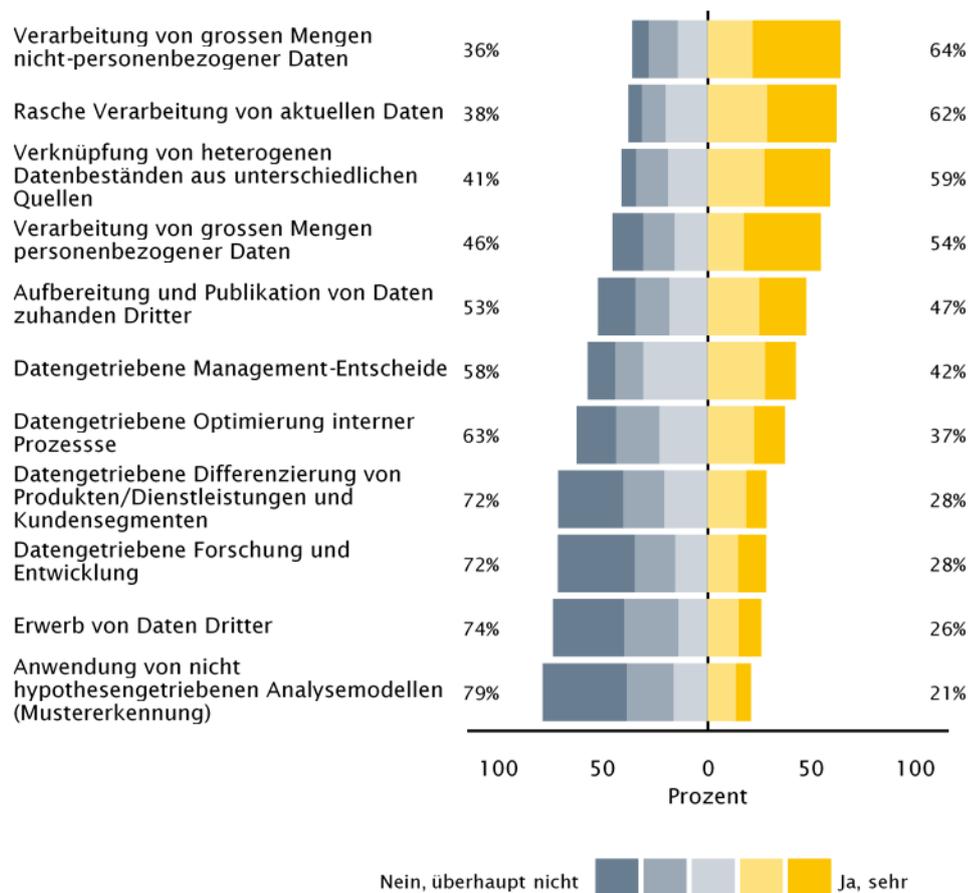


Abbildung 10: Datenbezogene Praktiken, welche im Unternehmen/in der Organisation eine wichtige Rolle spielen

Was die Art der Daten betrifft, die in grossen Mengen verarbeitet werden, werden die nicht-personenbezogenen Daten etwas häufiger genannt als die personenbezogenen. Bei den übrigen abgefragten Praktiken zeigt eine genauere Analyse, dass diese mit der Nennung der drei „V“ korrelieren, d.h. in jenen Unternehmen und Organisationen, in denen „Volume“, „Velocity“ und „Variety“ eine wichtige Rolle spielen, sind auch die übrigen Praktiken eher von Bedeutung: So bereiten 71% der Unternehmen/Organisation mit Big Data (im Sinne der 3 „V“) Daten zuhänden Dritter auf, während 43% dieser Unternehmen/Organisationen Daten von Dritten erwerben. Bei 62% spielen datengetriebene Management-Entscheidung eine wichtige Rolle, bei 52% die datengetriebene Optimierung interner Prozesse, bei 43% die datengetriebene Differenzierung von Produkten/Dienstleistungen und Kundensegmenten, bei 38% die datengetriebene Forschung und Entwicklung und schliesslich bei 34% die Anwendung von nicht-hypothesengetriebenen Analysemodellen (Mustererkennung). Damit lässt sich relativ gut charakterisieren, was ein Unternehmen mit „Big Data“ in der Schweiz aktuell ausmacht. Zugleich zeigen die Daten aber auch sehr schön auf, dass es sich bei „Big Data“ um ein graduelles Phänomen handelt: Viele Unternehmen und Organisationen sind zwar erst halbwegs in der Big-Data-Welt angekommen, haben es aber dennoch bereits heute mit verschiedenen Aspekten von Big Data zu tun.

## 7.4 Bedeutung von Big Data aus Sicht verschiedener Unternehmen / Organisationen

Anhand der Frage, ob die drei „V“ für das jeweilige Unternehmen bzw. für die jeweilige Organisation eine wichtige Rolle spielen, lässt sich ein ungefähres Bild von der Bedeutung von Big Data aus Sicht der verschiedenen Unternehmen / Organisationen zeichnen.

### 7.4.1 Bedeutung von Big Data für die verschiedenen Branchen

Abbildung 11 zeigt auf, inwieweit die drei „V“ in den Unternehmen bzw. Organisationen der Befragten eine wichtige Rolle spielen, aufgeschlüsselt nach Branchen. Dazu wird zur Messung der Bedeutung von Big Data eine Skala von 1 bis 4 verwendet: „0“ bedeutet, dass im betreffenden Unternehmen bzw. in der betreffenden Organisation bei der Datenverarbeitung weder „Volume“, noch „Variety“, noch „Velocity“ eine Rolle spielt, während am anderen Ende der Skala „3“ bedeutet, dass alle drei Aspekte eine wichtige Rolle spielen. Aus der Abbildung geht hervor, dass es in unserer Stichprobe hinsichtlich der Bedeutung von Big Data für die verschiedenen Branchen kaum nennenswerte Unterschiede gibt. Der einzige signifikante Unterschied besteht darin, dass es in der Branche „Unterrichtswesen, Forschung, Medien, Kultur“ mit 28% der Fälle etwas weniger oft vorkommt, dass alle drei „V“ eine wichtige Rolle spielen, als in den Branchen „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ (48%), „Management, Administration, Rechtswesen“ (43%) und „Technik, Informatik, Ingenieurwesen“ (40%). Zwischen dem öffentlichen Sektor und der Privatwirtschaft wurde kein signifikanter Unterschied hinsichtlich der Bedeutung von Big Data festgestellt. Diese Feststellungen gelten jedoch nur für die untersuchte Stichprobe und lassen sich nicht für alle Schweizer Unternehmen und Organisationen verallgemeinern. Verallgemeinernd festhalten lässt sich jedoch, dass es praktisch in allen Branchen Unternehmen oder Organisationen gibt, für die die verschiedenen Aspekte von Big Data eine wichtige Rolle spielen.

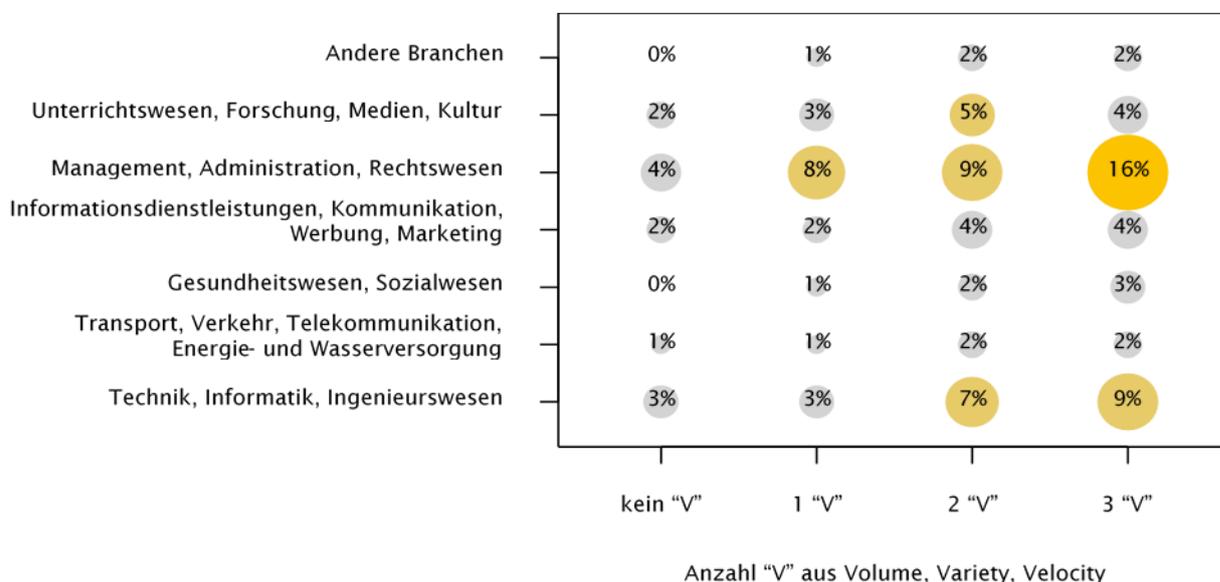


Abbildung 11: „Volume“, „Velocity“ und „Variety“ in den verschiedenen Branchen

## 7.4.2 Bedeutung von Big Data nach Grösse der Unternehmen / Organisationen

Wenn man die Unternehmen / Organisationen nach ihrer Grösse aufschlüsselt, so fällt auf, dass die Bedeutung von Big Data mit der Grösse des Unternehmens bzw. der Organisation korreliert: Während bei den in grossen Unternehmen / Organisationen Beschäftigten 47% angeben, dass alle drei „V“ für ihr Unternehmen / ihre Organisation eine wichtige Rolle spielen, sind es bei den in kleinen Einheiten (10-49 VZÄ) Beschäftigten nur 32% und bei den Mitarbeitenden von Kleinunternehmen bzw. Kleinstorganisationen mit weniger als 10 VZÄ gar nur 27% (siehe Abbildung 12).

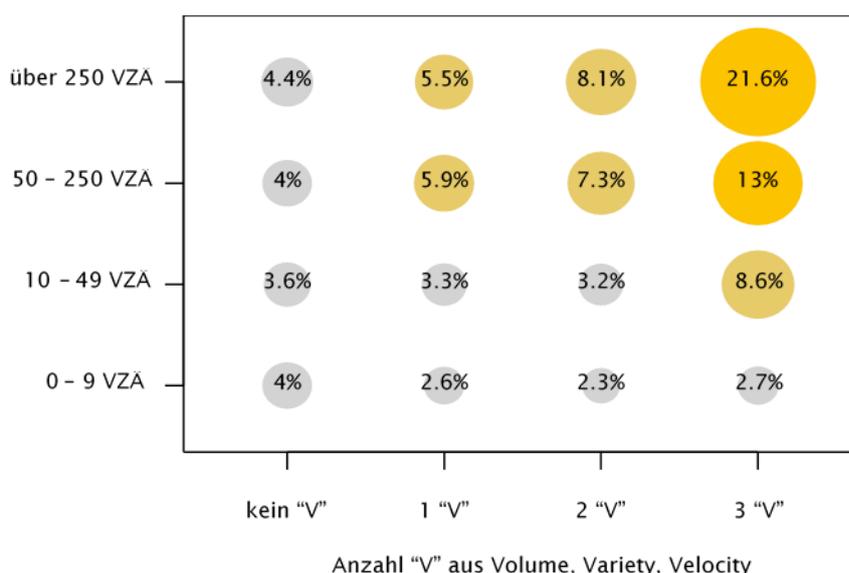


Abbildung 12: „Volume“, „Velocity“ und „Variety“ gemäss Grösse der Unternehmen/Organisationen

## 7.5 Chancen und Risiken von Big Data

Big Data birgt sowohl Chancen als auch Risiken: Abbildung 13 zeigt einen Überblick über die Bewertung der potentiellen Chancen von Big Data durch die Befragten, während Abbildung 14 Aufschluss über die Bewertung der Risiken gibt.

Was die positiven Aspekte von Big Data anbelangt, so sind rund 80% der Befragten der Ansicht, dass Big Data es ermöglicht, bisher unbekannte Zusammenhänge aufzudecken und neue Erkenntnisse zu gewinnen. Konkret wird Big Data von rund zwei Dritteln der Befragten als wichtiges Mittel gesehen, um genauere Prognosen und Risikoabschätzungen zu ermöglichen, um vermehrt daten- und faktenbasiert zu handeln, und um operative und logistische Abläufe zu optimieren. Eine Mehrheit der Befragten sieht zudem eine wichtige Chance von Big Data darin, dass es die Personalisierung von Informationen und Dienstleistungen und seitens von Organisationen und Unternehmen ein agileres Handeln ermöglicht. Etwas weniger überzeugt sind die Befragten von der Möglichkeit, dank Big Data Werbung zu personalisieren (48% Zustimmung; 37% Ablehnung), individuelle Preismodelle umzusetzen (47% Zustimmung; 31% Ablehnung) oder unter den Wirtschaftsakteuren „Schwarze Schafe“ (z.B. schlechte Zahler) frühzeitig zu identifizieren (39% Zustimmung; 35% Ablehnung). Dies dürfte nicht so sehr damit zu erklären sein, dass die Nutzung von Big Data für diese Zwecke aus Sicht der Befragten weniger gut denkbar wäre, sondern vielmehr damit, dass sie darin nicht nur Chancen, sondern auch erhebliche Risiken sehen.

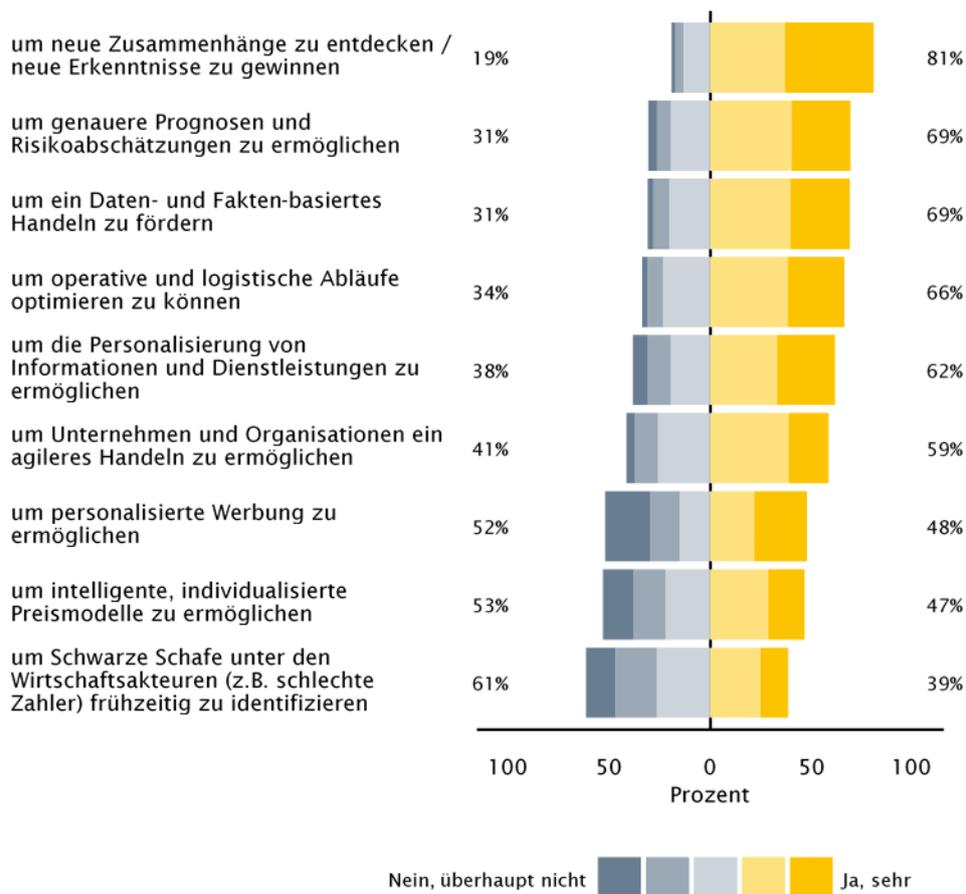


Abbildung 13: Bewertung der Chancen von Big Data

Bei den Risiken stehen die grundsätzliche Bedrohung der Privatsphäre und die missbräuchliche Verwendung von Daten, inklusive Datendiebstahl im Vordergrund. Rund 80% der Befragten sehen darin ein ernsthaftes Risiko von Big Data. Rund 60% der Befragten befürchten zudem, dass es aufgrund von Big Data beim Fällen von Entscheiden zu einer übertriebenen Fokussierung auf Daten kommt. Ebenso viele sind der Ansicht, dass Big Data eine erhöhte Gefahr von ökonomischer Diskriminierung mit sich bringt. Eine Reihe weiterer Risiken wird von rund der Hälfte der Befragten genannt: die unkontrollierte Eigendynamik der Systeme, die erhöhte Gefahr von persönlicher Repression (Stalking, Mobbing, Identitätsdiebstahl) und von Täuschungsdelikten, die Verschärfung von politischen und ökonomischen Machtgefällen sowie die erhöhte Gefahr von politischer Manipulation. Mit einer erhöhten Gefahr von staatlicher Repression rechnen hingegen nur 36% der Befragten, wobei diese Gefahr von jenen Befragten, die im privaten Sektor tätig sind, mit 45% Zustimmung (bei 27% Ablehnung) als ebenso hoch eingestuft wird wie die erhöhte Gefahr von persönlicher Repression.

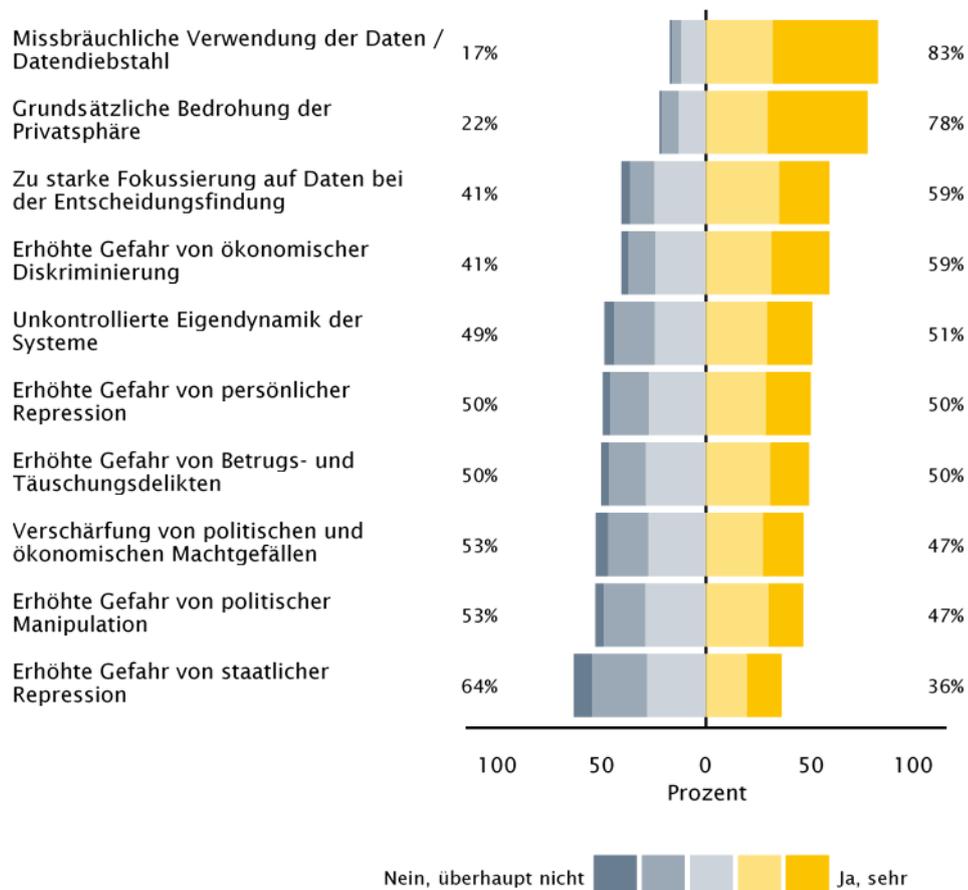


Abbildung 14: Bewertung der Risiken von Big Data

Interessanterweise tendieren jene Befragten, welche die Chancen von Big Data höher bewerten dazu, auch die Risiken höher zu bewerten. So machen die Big-Data-Enthusiasten, welche nur Chancen aber kaum Risiken sehen, weniger als 5% aus. Die Gruppe der reinen Big-Data-Pessimisten ist etwas grösser, beläuft sich aber auch auf deutlich weniger als 10% der Befragten. Die Befragten unterscheiden sich vielmehr darin, wie hoch sie das generelle Potential von Big Data (ob im Positiven oder im Negativen) einschätzen. Hier zeigt sich, dass etwa 2% der Befragten das Potential von Big Data als sehr gering einschätzen, rund ein Fünftel als gering, rund die Hälfte als mittel, wiederum rund ein Fünftel als hoch und etwa 5% als sehr hoch.

Die Befragten wurden gebeten, das Verhältnis von Chancen und Risiken aus persönlicher Sicht, aus Sicht ihres Arbeitgebers, aus Sicht ihrer Branche sowie (falls zutreffend) auch aus Sicht Ihres politischen bzw. zivilgesellschaftlichen Engagements zu bewerten. Dabei zeigt sich, dass Big Data aus persönlicher Sicht mit einem Durchschnitt von 3.4 Punkten auf einer Skala von 1 bis 5 etwas kritischer bewertet wird als aus Sicht des Arbeitgebers oder der Branche (3.8 bzw. 3.9 Punkte). Am negativsten wird Big Data jedoch aus Sicht des zivilgesellschaftlichen bzw. des politischen Engagements der Befragten bewertet (3.1 Punkte).

## 7.6 Vorstellungen hinsichtlich Datenschutz und Data Governance

Wie aus dem qualitativen Teil der Studie hervorgeht, bestehen bezüglich Datenschutz und Data Governance unterschiedliche Vorstellungen. Dank der Befragung können wir die verschiedenen Positionen nun quantifizieren.

### 7.6.1 Datenschutz

Im Rahmen der Expertenbefragung konnten hinsichtlich des Datenschutzes fünf verschiedene Ansätze unterschieden werden. Hierzu liefert die quantitative Erhebung folgende Ergebnisse (siehe Abbildung 15):

**Traditioneller Ansatz:** In seiner positiven Ausprägung („Besonders zu schützen sind Daten zu Gesundheit, finanzieller Situation, Religion, politischer Zugehörigkeit u.ä.“) genießt der traditionelle Ansatz eine fast einhellige Akzeptanz: 86% der Befragten stimmen der Aussage zu; weniger als 5% lehnen sie ab. In seiner negativen Ausprägung hingegen („Nicht besonders zu schützen sind Daten, die sowieso öffentlich sind, wie Name, Wohnort, Alter, Geschlecht.“) ist die Unterstützung für den traditionellen Ansatz vergleichsweise gering: Nur 44% der Befragten stimmen zu, während sich 39% dagegen aussprechen. Dies ist ein Hinweis darauf, dass die traditionelle Unterscheidung von besonders schützenswerten und weniger schützenswerten Daten für die Hälfte der Befragten keinen Sinn (mehr) ergibt.

**Big-Data-orientierter Ansatz:** Erklären lässt sich die halbherzige Unterstützung des traditionellen Ansatzes mit der Problematik, die mit der zunehmenden Verknüpfung verschiedenster Informationen einhergeht. So sind rund drei Viertel der Befragten der Ansicht, dass Daten, die es erlauben, jemanden zu identifizieren, besonders schützenswert sind, und dass das Verbinden von Personendaten aus verschiedenen Quellen in einem Personenprofil besonders problematisch ist.

**Ansatz der Unversehrtheit der digitalen Identität:** Beinahe einhellig (86% Zustimmung bei weniger als 5% Ablehnung) stellen sich die Befragten hinter die Forderung, dass die digitale Identität gleich zu schützen sei wie die physische; analog zur Garantie der physischen Unversehrtheit müssten auch die Daten, die einen betreffen, korrekt sein. Dem Aspekt der Richtigkeit der personenbezogenen Daten wird demnach eine sehr hohe Bedeutung zugemessen.

**Relativistische Ansätze:** 60% der Befragten sind der Ansicht, dass die Einschätzung, welche Daten schützenswert sind, individuell variiert und auch kulturell geprägt ist, während rund 20% gegenteiliger Meinung sind. Etwas weniger Zuspruch erhält mit 45% (bei 36% Ablehnung) die Aussage, dass eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Daten nicht sinnvoll sei, da die Frage, welche Daten schützenswert sind, kontextabhängig beantwortet werden müsse. Hier zeigt sich wiederum, dass rund die Hälfte der Befragten die traditionelle Unterscheidung zwischen mehr oder weniger schützenswerten Daten nicht für angemessen hält.

**Ansatz der persönlichen Datenhoheit:** Auflösen lässt sich die Frage der Einteilung von Information in mehr oder weniger schützenswerte Daten, indem man den Entscheid, welche Daten jemand wem zu welchem Zweck preisgeben möchte jedem/jeder Einzelnen überlässt. Die entsprechende Forderung stösst denn auch auf breite Zustimmung: 77% sprechen sich dafür aus; 9% sind dagegen.

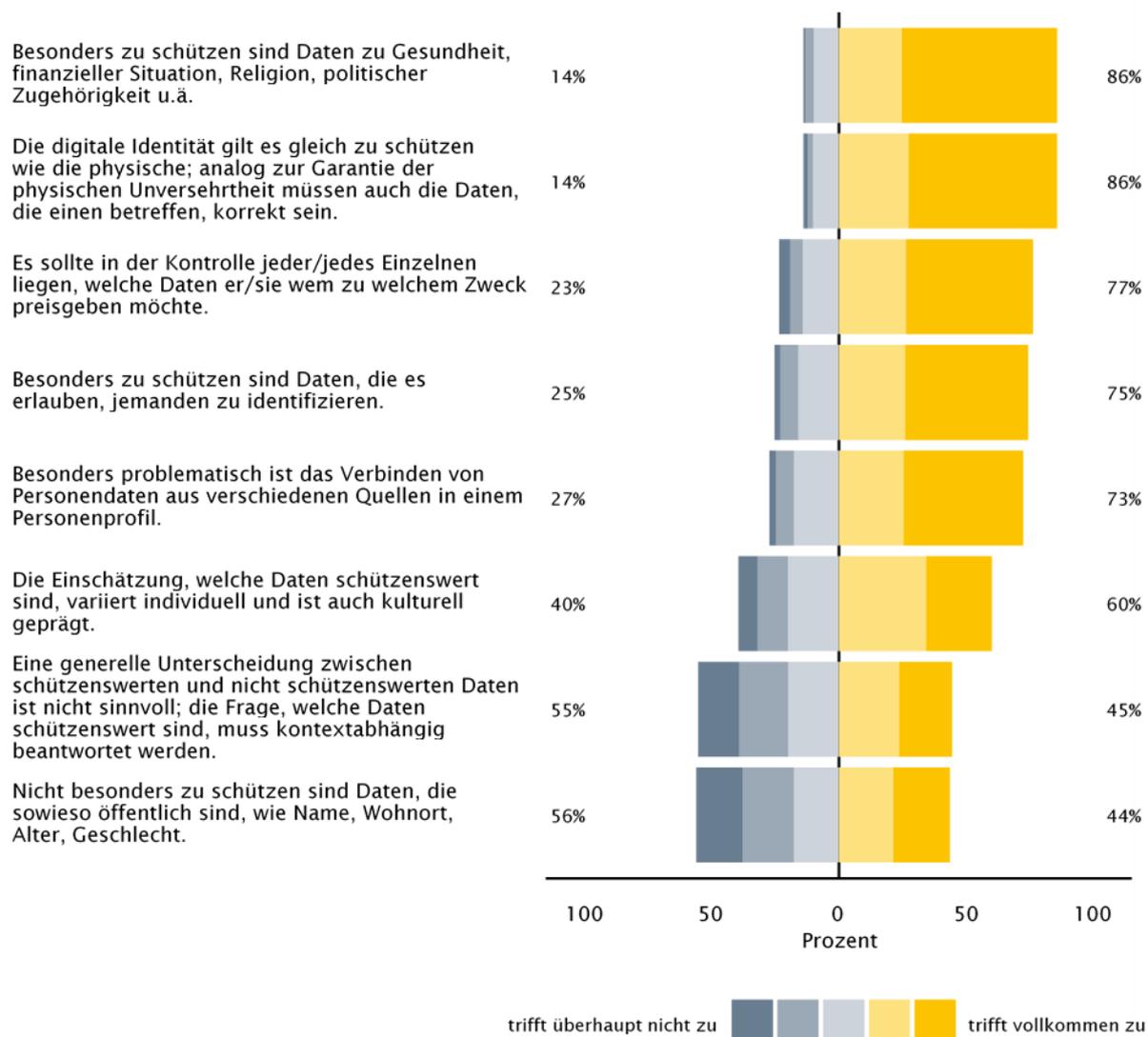


Abbildung 15: Vorstellung hinsichtlich der künftigen Ausgestaltung des Datenschutzes

### 7.6.2 Ausrichtung der künftigen Data-Governance

Eine weitere Frage der Umfrage diente dazu aufzuzeigen, wo die Befragten die Schwerpunkte der künftigen Data-Governance setzen würden. Dabei wurden sie angehalten, zwischen der privaten, persönlichen Sicht (inklusive der Sicht ihres persönlichen Umfeldes), der Sicht des Arbeitgebers und der Sicht ihres politischen bzw. zivilgesellschaftlichen Engagements zu unterscheiden. Um die Analyse weiter zu verfeinern, wurden die Antworten zudem dahingehend analysiert, von welchem Typ von Organisation die Befragten sprechen (Privatwirtschaft vs. öffentliche Hand; Anzahl Mitarbeitende) bzw. wofür sie sich im Rahmen ihres politischen oder zivilgesellschaftlichen Engagements einsetzen. Dabei zeigt sich, dass die folgenden drei Grundsätze quasi durchs Band auf Unterstützung zählen können:

**Prinzip der individuellen Datenhoheit (allgemein befürwortet):** Wie Abbildung 16 entnommen werden kann, wird das Prinzip der individuellen Datenhoheit aus persönlicher Perspektive allgemein sehr hoch gehalten (82% Zustimmung bei 7% Ablehnung). Aus Sicht der Unternehmen/Organisationen fällt die Zustimmung mit 69% deutlich geringer aus; das Item figuriert aber immerhin an zweiter Stelle (siehe Abbildung 17). Zwischen den einzelnen Organisationen gibt es aber deutliche Unterschiede: So tendieren Kleinunternehmen (0 bis 9 VZÄ) gemäss den Angaben ihrer Mitarbeitenden stärker dazu,

dem Prinzip der individuellen Datenhoheit zuzustimmen (84% Zustimmung) als öffentlich-rechtliche Organisationen (66%) oder Privatunternehmen mit über 250 Mitarbeitenden (61%). Betrachtet man die einzelnen Branchen, so fällt die Zustimmung im Bereich „Sozialwesen, Gesundheitswesen“ mit 81% am stärksten aus, während sie am anderen Ende des Spektrums im Bereich „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ 61% beträgt. Die stärkste Zustimmung erhält das Prinzip der individuellen Datenhoheit mit 88% jedoch aus der Perspektive des politischen bzw. zivilgesellschaftlichen Engagements der Befragten (siehe Abbildung 18). Dabei weisen jene Befragten, welche sich für den Konsumentenschutz (98% Zustimmung), das Recht auf informationelle Selbstbestimmung (94%) und den Datenschutz (93%) einsetzen, die höchsten Zustimmungsraten auf.

**Datenschutz dank technischen Massnahmen (allgemein befürwortet):** Ein breiter Konsens herrscht auch bezüglich der Forderung, dass der Datenschutz durch technische Massnahmen sicherzustellen sei: Drei Viertel der Befragten stimmen aus persönlicher Sicht zu (75% Zustimmung bei 8% Ablehnung); ebenso gross ist die Zustimmung aus Sicht der Unternehmen/Organisationen (75%) und des politischen bzw. zivilgesellschaftlichen Engagements (74%). Die höchsten Zustimmungsraten weisen jene Befragten auf, welche sich für den Konsumentenschutz (93%) bzw. für das Recht auf informationelle Selbstbestimmung (82%) einsetzen, gefolgt von den Unternehmen und Organisationen im Bereich „Gesundheitswesen, Sozialwesen“ (81%).

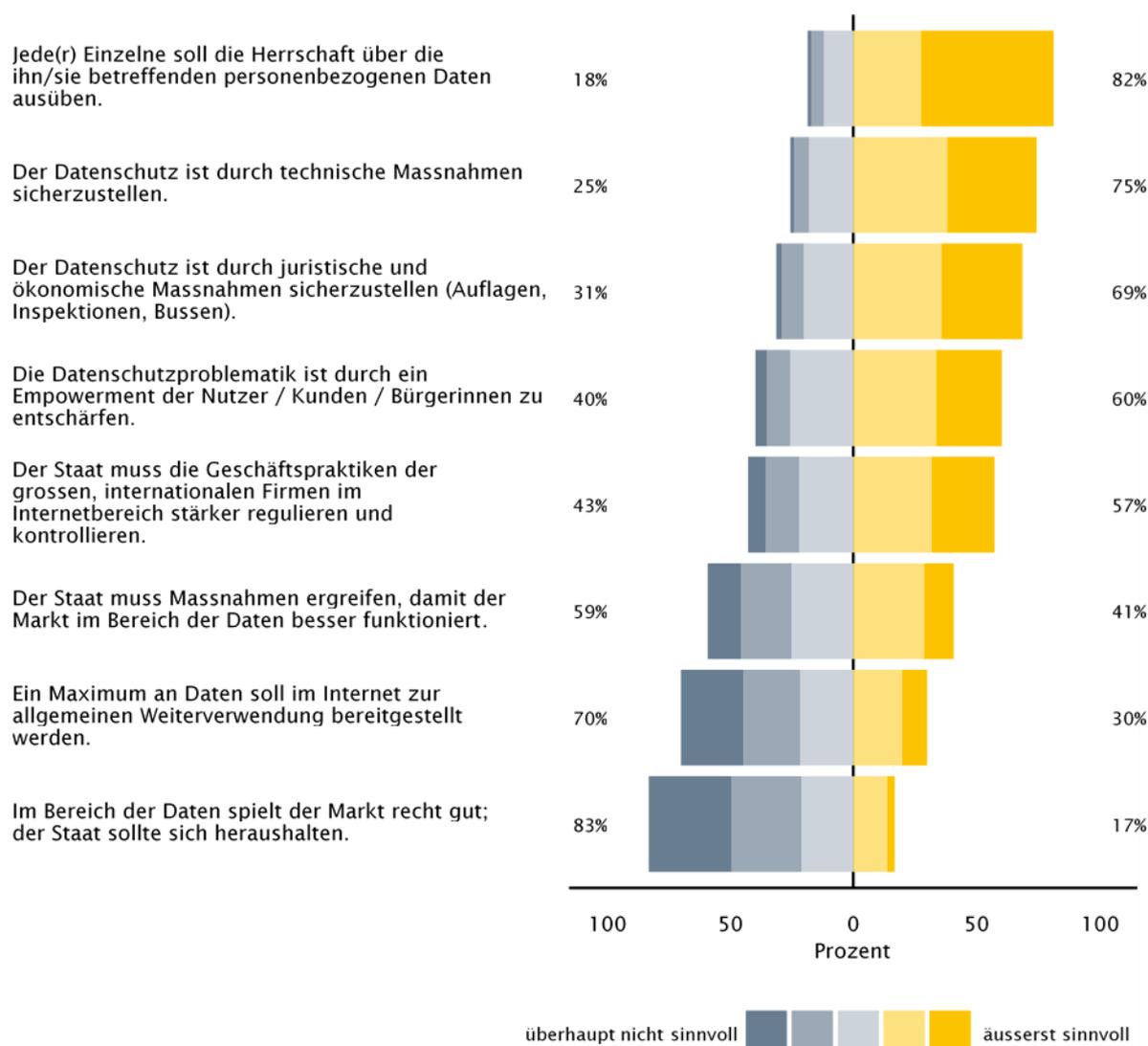


Abbildung 16: Schwerpunkte der künftigen Data-Governance aus persönlicher Sicht

### Datenschutz durch Empowerment der Nutzer / Kunden / Bürgerinnen (allgemein befürwortet):

Auch die Forderung, dass die Datenschutzproblematik durch ein Empowerment der Nutzer / Kunden / Bürgerinnen zu entschärfen sei, wird generell gutgeheissen. Drei Fünftel der Befragten stimmen aus persönlicher Sicht zu (60% Zustimmung bei 14% Ablehnung). Noch höher fällt die Zustimmungsrate aus der Sicht des politischen oder zivilgesellschaftlichen Engagements der Befragten aus (72%), während sie aus der Sicht der Unternehmen/Organisationen mit 55% etwas niedriger ausfällt. Interessanterweise fällt die Zustimmungsrate bei den grossen öffentlich-rechtlichen Organisationen (über 250 VZÄ) höher aus als bei den mittleren Organisationen des öffentlichen Sektors (59% vs. 46%), während sie bei den Kleinstunternehmen (0-9 VZÄ) höher ausfällt als bei den Kleinunternehmen (10-49 VZÄ) (67% vs. 47%). Einen eindeutigen Zusammenhang zwischen Grösse und Zustimmungsrate lässt sich jedoch weder für den öffentlichen noch für den privaten Sektor feststellen. Aus politischer bzw. zivilgesellschaftlicher Perspektive weisen jene Befragten die höchsten Zustimmungsraten auf, welche sich für den freien Zugang zu Wissen (78%) einsetzen.

Während die drei vorangehenden Grundsätze kaum auf Widerstand stossen, bietet sich bei den folgenden beiden Ansätzen ein differenzierteres Bild: Sie werden von den meisten Akteuren befürwortet, allen voran vom Konsumentenschutz. Bei den Grossunternehmen dürften sie aber kaum auf Anklang stossen.

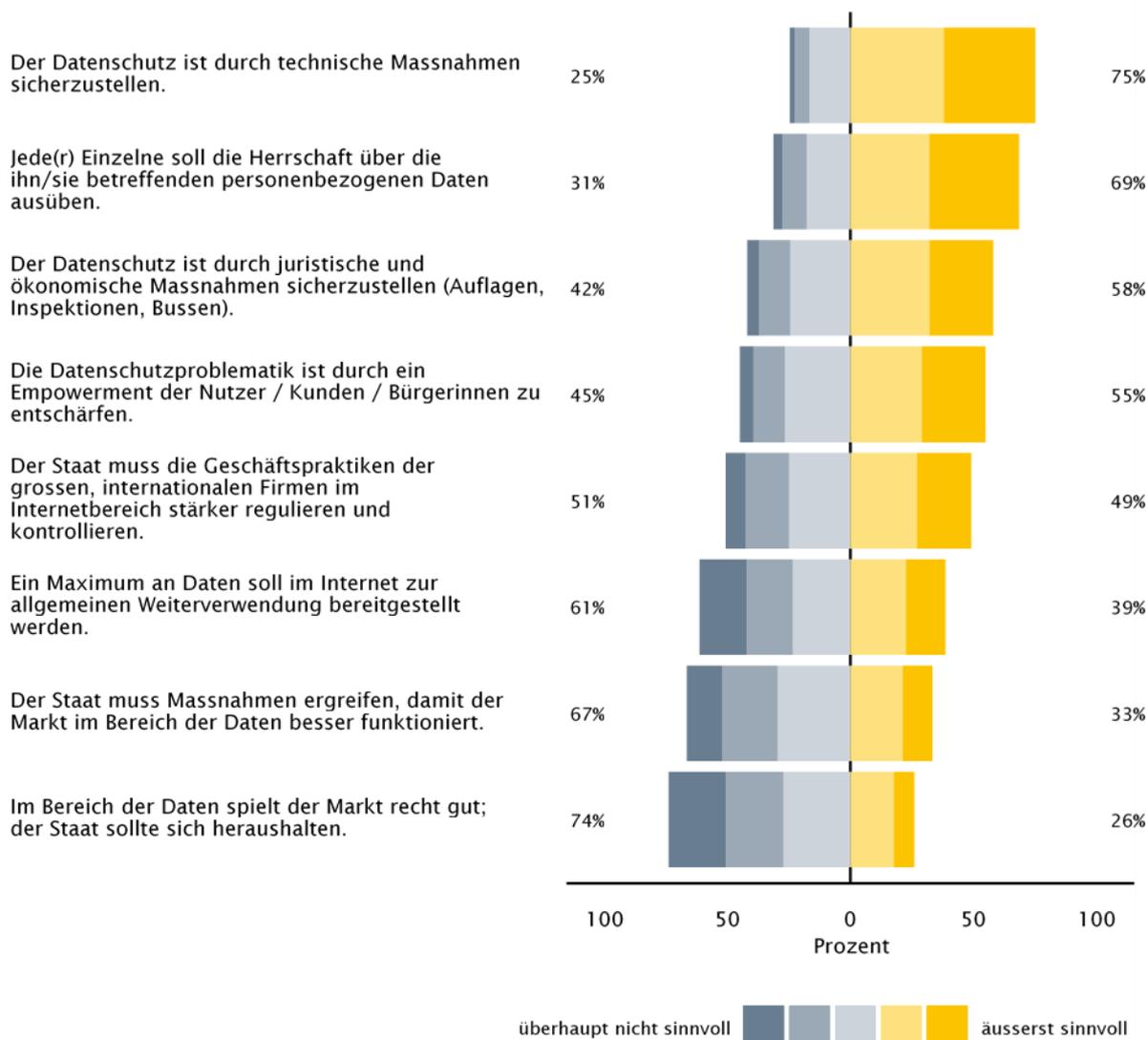


Abbildung 17: Schwerpunkte der künftigen Data-Governance aus Sicht des Arbeitgebers

**Datenschutz dank juristischen und ökonomischen Massnahmen (vorwiegend befürwortet, von Grossunternehmen abgelehnt):** Die Forderung, dass der Datenschutz durch juristische und ökonomische Massnahmen (Auflagen, Inspektionen, Bussen) sicherzustellen sei, wird von den Befragten fast durchs Band gutgeheissen: Über zwei Drittel der Befragten stimmen aus persönlicher Sicht zu (69% Zustimmung bei 11% Ablehnung). Ebenso hoch ist die Zustimmungsrate aus der Perspektive des politischen oder zivilgesellschaftlichen Engagements der Befragten (68%), während sie aus der Sicht der Unternehmen/Organisationen mit 58% wiederum etwas niedriger ausfällt. Ein genauerer Blick auf die Unternehmen/Organisationen zeigt, dass diese Maxime bei den öffentlich-rechtlichen Organisationen auf stärkere Zustimmung stösst als bei den privatwirtschaftlichen Unternehmen (63% vs. 48% Zustimmung). Bei diesen wiederum ist die Grösse ausschlaggebend: Je grösser das Unternehmen, desto geringer die Zustimmungsrate. Während Kleinunternehmen (0-9 VZÄ) mit 62% in etwa dieselbe Zustimmungsrate aufweisen wie die öffentlich-rechtlichen Organisationen, beträgt sie für Grossunternehmen nur 31%. Auch bei den Branchen gibt es Unterschiede: Die höchsten Zustimmungsraten weisen die Bereiche „Gesundheitswesen, Sozialwesen“ (70%) und „Management, Administration, Rechtswesen“ (63%) auf, während sie in den Bereichen „Technik, Informatik, Ingenieurwesen“ (53%) und „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (51%) nur knapp über der 50%-Marke liegen. Aus politischer bzw. zivilgesellschaftlicher Perspektive weisen jene Befragten die höchsten Zustimmungsraten auf, welche sich für den Konsumentenschutz (93%) oder den Datenschutz (73%) einsetzen.

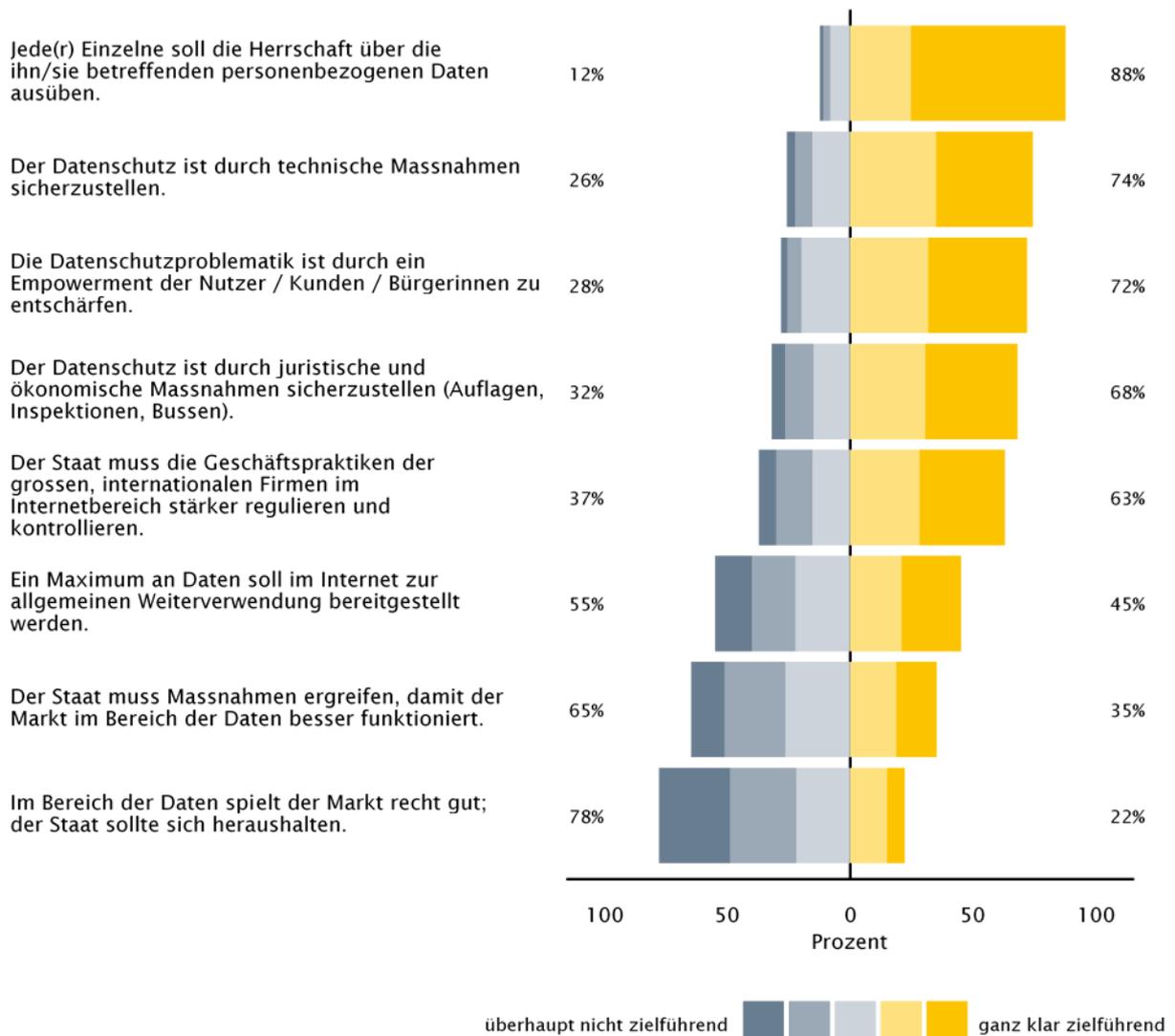


Abbildung 18: Schwerpunkte der künftigen Data-Governance aus zivilgesellschaftlicher Sicht

**Stärkere Regulierung und Kontrolle der Geschäftspraktiken der Internet-Riesen (vorwiegend befürwortet, von Grossunternehmen abgelehnt):** Über die Hälfte der Befragten fordert aus persönlicher Sicht eine stärkere Regulierung und Kontrolle der Geschäftspraktiken der grossen, internationalen Firmen im Internetbereich durch den Staat (57% Zustimmung bei 21% Ablehnung). Etwas höher ist die Zustimmungsrates aus der Perspektive des politischen oder zivilgesellschaftlichen Engagements der Befragten (63%), während sie aus der Sicht der Unternehmen/Organisationen mit 49% niedriger ausfällt. Dabei fällt wiederum auf, dass die Forderung bei den öffentlich-rechtlichen und den Nonprofit-Organisationen eher auf Zustimmung stösst als bei den privatwirtschaftlichen Unternehmen. Und bei diesen ist wiederum die Grösse ausschlaggebend: Je grösser das Unternehmen, desto geringer die Zustimmungsrates. Während Kleinstunternehmen (0-9 VZÄ) mit 52% dieselbe Zustimmungsrates aufweisen wie die öffentlich-rechtlichen Organisationen, beträgt diese für Grossunternehmen nur 25%. Aber auch bei den Branchen gibt es Unterschiede: Hier weist der Bereich „Gesundheitswesen, Sozialwesen“ mit 62% die höchste Zustimmungsrates auf, während die Unternehmen und Organisationen aus den Bereichen „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ (37%), „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (42%), sowie „Technik, Informatik, Ingenieurwesen“ (45%) dieser Forderung eher kritisch gegenüber stehen. Aus politischer bzw. zivilgesellschaftlicher Perspektive weisen jene Befragten die höchste Zustimmungsrates auf, welche sich für den Konsumentenschutz (93%) einsetzen.

Die letzten beiden Ansätze sind umstritten, wobei sich die Pro- und Contra-Stimmen in etwa die Waage halten:

**Staatliche Intervention am Datenmarkt (umstritten):** Inwieweit es staatlicher Interventionen am Datenmarkt bedarf, wurde mittels zweier Items abgefragt. Dabei stiess die Aussage, dass der Markt im Bereich der Daten recht gut spiele und sich der Staat daher heraushalten solle, gemeinhin auf Ablehnung. Am stärksten fiel diese aus der persönlichen Sicht der Befragten aus (62% Ablehnung; 17% Zustimmung), gefolgt von der Perspektive des politischen oder zivilgesellschaftlichen Engagements (56% Ablehnung; 22% Zustimmung) und der Sicht der Unternehmen/Organisationen (47% Ablehnung; 26% Zustimmung). Die höchsten Zustimmungsrates weisen die Privatwirtschaft (37%) und die Non-Profit-Organisationen<sup>7</sup> (41%) auf. Dabei ist auch hier die Zustimmungsrates wiederum abhängig von der Grösse der Unternehmen: Je grösser das Unternehmen, desto höher die Zustimmungsrates. Während sie bei den Grossunternehmen 55% beträgt, beläuft sie sich bei den Kleinstunternehmen nur auf 28%. In den verschiedenen Branchen liegen die Zustimmungsrates zwischen 20% und 37%. Aus politischer bzw. zivilgesellschaftlicher Perspektive weisen jene Befragten die geringste Zustimmungsrates auf, welche sich für den Konsumentenschutz einsetzen (7% Zustimmung), während sich die Vertreter von Brancheninteressen (50% Zustimmung) auf der Seite der Grossunternehmen einreihen. Während sich demnach bei diesem ersten, negativ formulierten Item dasselbe Bild zeichnet wie bei den beiden vorangehenden Ansätzen, fällt die Einschätzung dann doch etwas zögerlicher aus, wenn es um die explizite Forderung geht, dass der Staat Massnahmen ergreifen soll, damit der Markt im Bereich der Daten besser funktioniert: Hier fällt die Zustimmung aus persönlicher Sicht bei 41% Zustimmung und 34% Ablehnung weit verhaltener aus. Aus Sicht des politischen und zivilgesellschaftlichen Engagements der Befragten (35% Zustimmung; 39% Ablehnung) sowie aus der Perspektive der Unternehmen/Organisationen (33% Zustimmung; 37% Ablehnung) stösst die Forderung eher auf Ablehnung. Erwartungsgemäss fällt hier die Zustimmungsrates der Privatwirtschaft mit 27% geringer aus als jene des öffentlichen Sektors (34%). Mehrheitlich befürwortet wird die Forderung nach staatlicher Intervention am Datenmarkt indessen aus Sicht des Konsumentenschutzes (55%). Eine knappe Zustimmung erfährt sie auch seitens der Unternehmen und Organisationen im Bereich „Gesundheitswesen, Sozialwesen“ (51%), während andere Branchen davon weit weniger halten.

**Generelle Anwendung des Open-Data-Prinzips (umstritten):** Ebenso umstritten ist die Forderung, dass ein Maximum an Daten im Internet zur allgemeinen Weiterverwendung bereitgestellt werden soll. Dieser Verallgemeinerung des Open-Data-Prinzips, von der nicht nur die Daten der Privatwirtschaft, sondern insbesondere auch grosse Mengen von personenbezogenen Daten betroffen wären, stimmen

<sup>7</sup> Bei den in unserer Stichprobe enthaltenen Nonprofit-Organisationen dürfte es angesichts der Umfrageergebnisse zu einem guten Teil um Lobby-Organisationen handeln, die Unternehmen als Instrumente dienen, um einen kommerziellen Zweck zu verfolgen. Die Ergebnisse sollten daher nicht auf den klassischen Nonprofit-Sektor (gemeinnützige Organisationen gemäss der landläufigen Definition des Begriffs) extrapoliert werden.

die Befragten aus Sicht ihres politischen bzw. zivilgesellschaftlichen Engagements (45% Zustimmung; 33% Ablehnung) noch am ehesten zu, während sich Pro und Contra aus der Perspektive der Organisationen/Unternehmen (39% Zustimmung; 38% Ablehnung) in etwa die Waage halten und das Verdikt aus persönlicher Sicht (30% Zustimmung; 49% Ablehnung) negativ ausfällt. Dabei ist allerdings anzumerken, dass die Forderung bei der Privatwirtschaft (46%) noch eher auf Anklang stösst als im öffentlichen Sektor (35%) und dass die politischen und zivilgesellschaftlichen Akteure gespalten sind: Aus Sicht des Datenschutzes wird die Forderung verhalten aufgenommen (39% Zustimmung), während sie von den Befragten, welche sich für den freien Zugang zu Wissen und die Weiterverwendung von nicht-personenbezogenen Daten (Open Data) einsetzen, bei Zustimmungsraten von knapp über 50 Prozent unterstützt wird.

Da die Befragten gebeten wurden, zu den verschiedenen Items aus unterschiedlicher Perspektive Stellung zu nehmen, lässt sich auf der Ebene der betroffenen Personen die Dissonanz zwischen den verschiedenen Sichten hinsichtlich der Wünschbarkeit der einzelnen Ansätze eruieren. Hierzu wurden die Antworten aus der menschenzentrierten Perspektive (Perspektive der persönlichen Situation und jener des persönlichen Umfelds der Befragten) mit jenen aus der organisationszentrierten Perspektive und jenen aus der Perspektive des politischen bzw. zivilgesellschaftlichen Engagements in Beziehung gesetzt. Dabei zeigt sich, dass das Ausmass der Dissonanz je nach Wirtschaftssektor, Unternehmensgrösse, Interessengruppe und Thema unterschiedlich stark ausfällt:

**Organisationsperspektive versus menschenzentrierte Sicht:** Wenn die Organisationsperspektive mit der persönlichen Perspektive in Beziehung gesetzt wird, ist die grösste Dissonanz bei den Mitarbeitenden von Grossfirmen und von Nonprofit-Organisationen mit Blick auf das Item „Im Bereich der Daten spielt der Markt recht gut; der Staat sollte sich heraushalten“ festzustellen. Bei den Grossfirmen beträgt die durchschnittliche Dissonanz auf der Skala von 1-5 einen ganzen Punkt; bei den Nonprofit-Organisationen immerhin 0.78 Punkte. Mit anderen Worten: Zwischen der persönlichen Sicht der Befragten und der Sicht der betroffenen Unternehmen tut sich ein beträchtlicher Hiatus auf, denn auch die Mitarbeitenden von Grossunternehmen sind persönlich eher der Meinung, dass der Markt im Bereich der Daten nicht spielt (45% lehnen das Item ab, während nur 22% zustimmen; aus Sicht der Grossunternehmen beläuft sich die Zustimmungsraten dagegen auf 55%). Mit sinkender Unternehmensgrösse nimmt die Dissonanz mit Blick auf dieses Item ab: Bei den Mitarbeitenden von mittleren Unternehmen beträgt sie noch 0.64 Punkte, bei jenen von kleinen Unternehmen 0.58 Punkte und bei jenen von Kleinstunternehmen 0.28 Punkte – ein Wert, der mit jenem der Mitarbeitenden von grossen Organisationen des öffentlichen Sektors (0.30 Punkte) vergleichbar ist. Praktisch dasselbe Muster, wenn auch etwas weniger ausgeprägt und zum Teil mit umgekehrtem Vorzeichen, ist auch für die Items „Der Datenschutz ist durch juristische und ökonomische Massnahmen sicherzustellen (Auflagen, Inspektionen, Bussen)“, „Ein Maximum an Daten soll im Internet zur allgemeinen Weiterverwendung bereitgestellt werden“ und „Der Staat muss die Geschäftspraktiken der grossen, internationalen Firmen im Internetbereich stärker regulieren und kontrollieren“ zu beobachten. Hier beträgt die Dissonanz bei den Mitarbeitenden der Grossfirmen jeweils rund 0.7 Punkte. Dies ist ein weiterer Hinweis darauf, dass die Geschäftsinteressen von grösseren Unternehmen im Umgang mit Daten teilweise den Nutzer- und Konsumenteninteressen entgegenlaufen. Aber auch der öffentliche Sektor ist von solchen Dissonanzen nicht ganz gefeit: Hinsichtlich des Prinzips der individuellen Datenhoheit, das aus persönlicher Sicht der Befragten auf eine sehr hohe Zustimmung stösst, beträgt die Dissonanz bei den Mitarbeitenden von mittleren Organisationen des öffentlichen Sektors (50-250 VZÄ) immerhin einen halben Punkt; übertroffen werden sie diesbezüglich nur von den Mitarbeitenden der Grossunternehmen mit einer Abweichung von 0.63 Punkten.

**Perspektive des politischen oder zivilgesellschaftlichen Engagements versus menschenzentrierte Sicht:** Indem die Perspektive des politischen bzw. zivilgesellschaftlichen Engagements mit der persönlichen Perspektive in Beziehung gesetzt wird, lässt sich aufzeigen, welche Interessengruppen Ansichten vertreten, die aus Sicht ihrer Vertreterinnen und Vertreter von einer menschenzentrierten Sicht abweichen. Hier fallen die Dissonanzen im Vergleich zur Sicht der meisten Interessengruppen geringer aus als beim Vergleich mit der Organisationssicht. Die grosse Ausnahme bilden jene Befragten, welche Brancheninteressen vertreten. Bei der Frage, ob der Markt im Bereich der Daten recht gut spielt und der Staat sich daher heraushalten sollte, beträgt die Abweichung ganze 1.17 Punkte und beim Item „Die Datenschutzproblematik ist durch ein Empowerment der Nutzer / Kunden / Bürgerinnen zu entschärfen“ 0.69 Punkte. Bei der Frage, ob der Markt im Bereich der Daten recht gut spielt, ist zudem auch bei den Vertretern der Standortförderung eine Abweichung von 0.56 Punkten

festzustellen. Bei den übrigen Items und Interessengruppen beträgt die Dissonanz jeweils weniger als einen halben Punkt.

### 7.6.3 Der Wert von Daten und die Preisbildung am Daten-Markt

Da im Rahmen der Expertenbefragung bezüglich der Funktionsweise des Datenmarkts scheinbar widersprüchliche Aussagen gemacht wurden, wurde dieser Aspekt in der quantitativen Erhebung mittels einer separaten Frage nochmals gezielt thematisiert. Wie der Abbildung 19 entnommen werden kann, besteht unter den Umfrageteilnehmern beinahe Einhelligkeit darüber, dass der Datenmarkt aktuell in verschiedener Hinsicht versagt. Betrachtet man das Ergebnis der Austauschverhältnisse auf dem sogenannten Datenmarkt, so lautet das Fazit mehrheitlich, dass die Leute generell für die Preisgabe ihrer Daten keine faire Gegenleistung erhalten. 76% vertreten diese Ansicht in Bezug auf die Preisgabe von Daten im Internet (bei 9% Gegenstimmen) und 68% in Bezug auf die Preisgabe von Daten ausserhalb des Internets (bei 8% Gegenstimmen). Wenn wir uns die Ursachen für diese Schiefelage ansehen, fällt auf, dass das grösste Problem im Machtungleichgewicht zwischen Kunden/Nutzern und Anbietern verortet wird (80% der Befragten sind dieser Ansicht); dabei sind knapp zwei Drittel der Befragten der Ansicht, dass der Datenmarkt aufgrund von Informations-Asymmetrien und aufgrund von natürlichen Monopolen in etlichen Bereichen versagt (weniger als 15% der Befragten sind hier jeweils gegenteiliger Meinung). Gut die Hälfte der Befragten erachtet es zudem aus gesellschaftlicher Sicht für problematisch, wenn zu viele Menschen ihre persönlichen Daten aus individuellen Nutzenüberlegungen heraus preisgeben (rund ein Viertel findet, dass dies nicht der Fall ist).

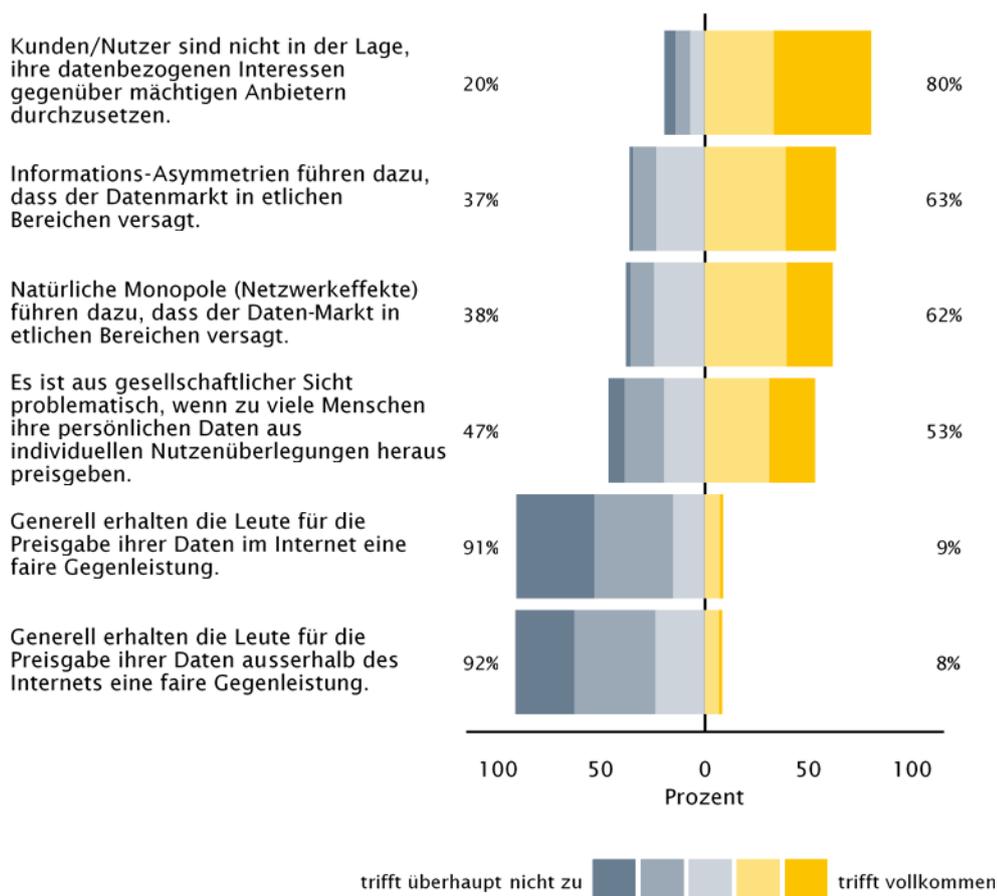


Abbildung 19: Der Wert von Daten und die Preisbildung am Daten-Markt

## 7.7 Kollektiver Handlungsbedarf

Schliesslich wollten wir von den Befragten wissen, in welchen Bereichen sie kollektiven Handlungsbedarf verorten, um sicherzustellen, dass die positiven Seiten von Big Data zum Tragen kommen und die Risiken minimiert werden.

### 7.7.1 Prioritäre Handlungsfelder

Den Abbildungen 20 und 21 kann entnommen werden, in welchen Bereichen die Befragten den grössten Handlungsbedarf ausmachen. Die Umfrageergebnisse legen nahe, dass sieben Handlungsfelder mit hoher Priorität angegangen werden sollten. Da einzelne Massnahmen in den verschiedenen Handlungsfeldern ähnlich hohe Zustimmungsraten erzielten (zwischen 64% und 75% Zustimmung), wird auf eine weitere Priorisierung der Handlungsfelder verzichtet. Eine Priorisierung sollte hingegen innerhalb der einzelnen Handlungsfelder erfolgen, denn nicht alle vorgeschlagenen Massnahmen erhielten seitens der Umfrageteilnehmer denselben Zuspruch. Da einige der Massnahmen seitens der Mitarbeitenden des öffentlichen Sektors und jenen der Privatwirtschaft unterschiedlich eingeschätzt werden und jene der Privatwirtschaft in der Stichprobe stark untervertreten sind, wird jeweils angemerkt, falls ein nennenswerter Zusammenhang mit dem Beschäftigungssektor festgestellt werden konnte. Dabei wird die Organisationsgrösse auch gleich mit berücksichtigt.

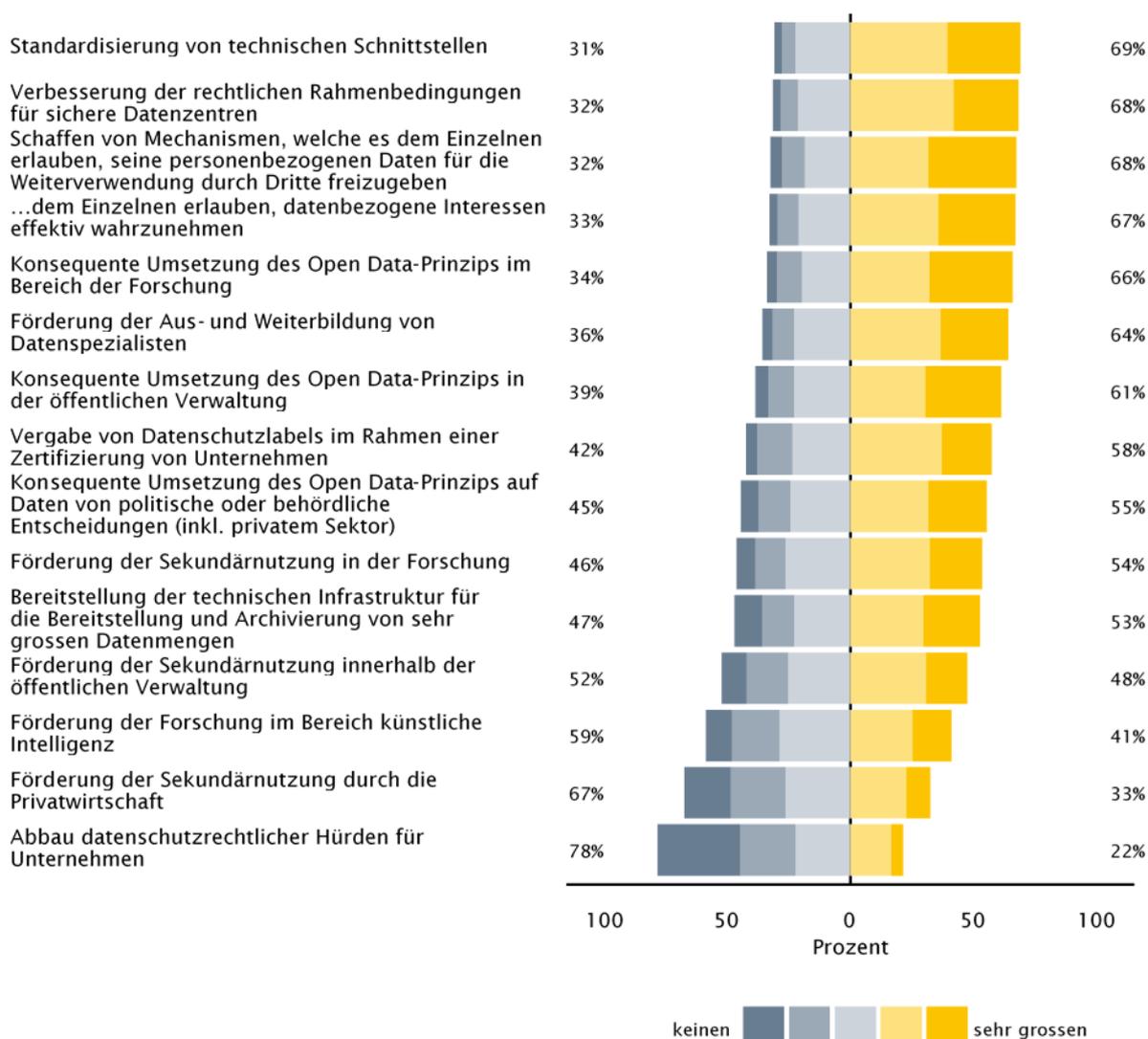


Abbildung 20: Handlungsbedarf, um sicherzustellen, dass die positiven Seiten von Big Data zum Tragen kommen.

### Empowerment der Nutzerinnen und Nutzer mit Blick auf die Kontrolle von personenbezogenen

**Daten:** Durch die verstärkte Kontrolle der Nutzerinnen und Nutzer über ihre eigenen Daten sollen sowohl Chancen von Big Data besser genutzt als auch Risiken vermindert werden. Um ein solches Empowerment zu ermöglichen, sind neue Eigentums- oder Nutzungsrechte im Bereich der personenbezogenen Daten zu definieren (75% Zustimmung), Mechanismen zu schaffen, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben (68% Zustimmung) und Dienste bereitzustellen, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen (67% Zustimmung). Dieser Kategorie lässt sich auch die Förderung der Entwicklung von Lösungen zur Verbesserung der Human-Data-Interaktion zuordnen. Allerdings verorten hier nur 55% der Befragten Handlungsbedarf.

Im Vergleich zu den Mitarbeitenden des öffentlichen Sektors befürworteten Mitarbeitende von Privatunternehmen eher, dass Mechanismen geschaffen werden, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben (75% vs. 64% Zustimmung). Unter den Mitarbeitenden des öffentlichen Sektors stimmen jene von grösseren Organisationen eher zu als jene von mittleren und kleinen (69% vs. 55-57% Zustimmung); im privaten Sektor ist kein solcher Grösseneffekt zu beobachten.

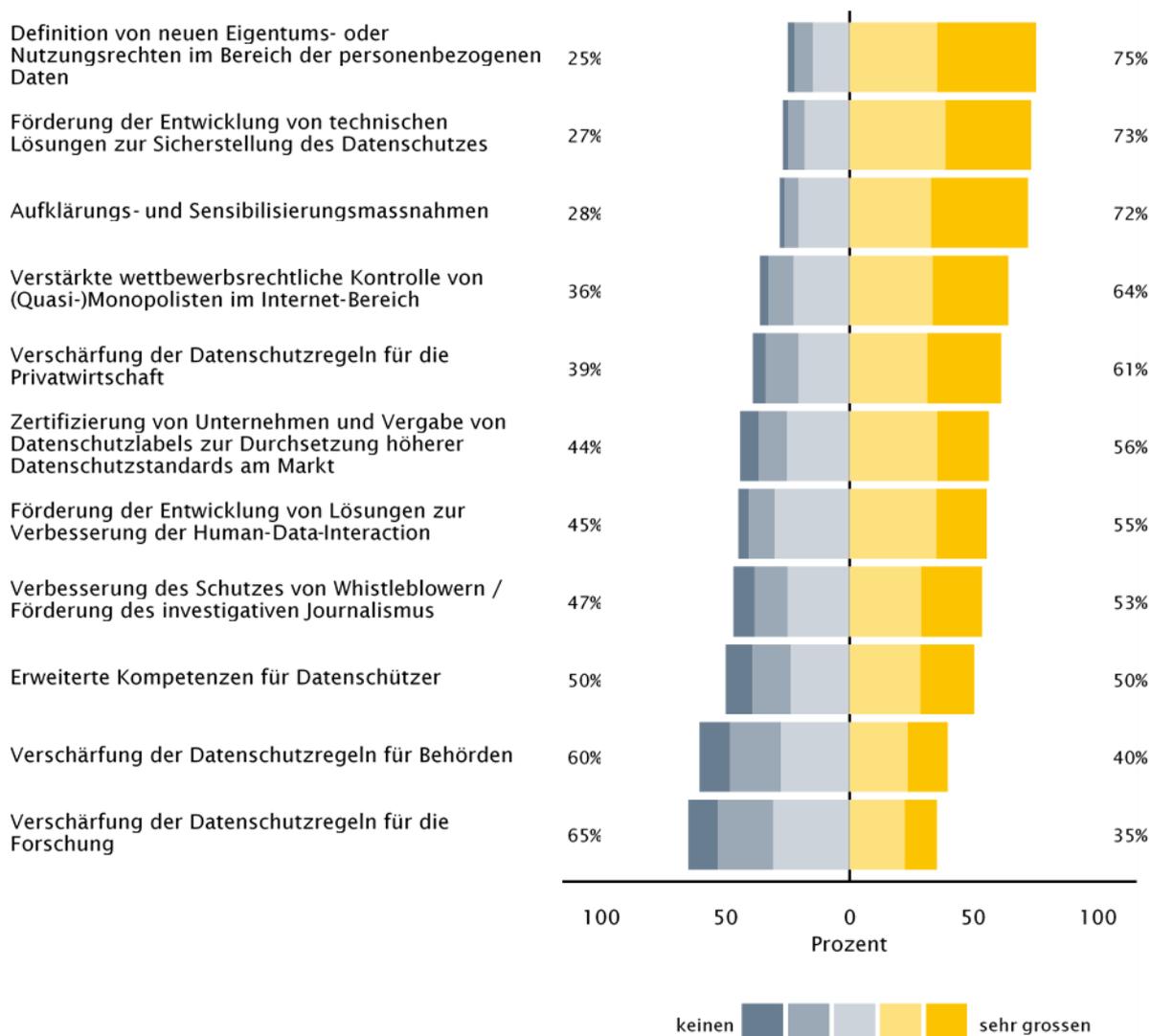


Abbildung 21: Handlungsbedarf, um sicherzustellen, dass die Risiken von Big Data minimiert werden

**Verbesserung des Datenschutzes:** Um die Risiken von Big Data zu vermindern, soll der Datenschutz verbessert werden. Dies soll in erster Linie entlang von zwei Dimensionen geschehen – einerseits soll die Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes gefördert werden (73% Zustimmung), und andererseits braucht es Aufklärungs- und Sensibilisierungsmassnahmen (72% Zustimmung). Weitere Massnahmen, welche mindestens die Hälfte der Befragten als wichtig erachten, umfassen die Verschärfung der Datenschutzregeln für die Privatwirtschaft (61% Zustimmung), die Zertifizierung von Unternehmen/Organisationen und die Vergabe von Datenschutzlabels (56% bzw. 58% Zustimmung) sowie erweiterte Kompetenzen für Datenschutzbeauftragte (50% Zustimmung). Klar ist auch, dass die datenschutzrechtlichen Hürden für Unternehmen nicht abgebaut werden sollten (56% der Befragten lehnen einen entsprechenden Abbau von Hürden ab). Umstritten ist, ob die Datenschutzregeln auch für die Behörden (40% Zustimmung; 33% Ablehnung) und die Forschung (35% Zustimmung; 34% Ablehnung) verschärft werden sollen.

Erwartungsgemäss sprechen sich Mitarbeitende des öffentlichen Sektors stärker für eine Verschärfung der Datenschutzregeln für die Privatwirtschaft aus als Umfrageteilnehmer, die selber in der Privatwirtschaft tätig sind (65% vs. 51% Zustimmung). Allerdings ist die Haltung der in der Privatwirtschaft Tätigen auch von der Grösse des Unternehmens abhängig. So stimmen Mitarbeitende von Kleinunternehmen der Forderung mehrheitlich zu (60% Zustimmung), während Mitarbeitende von Grossfirmen hier kaum Handlungsbedarf verorten (38% Zustimmung). Interessanterweise ist die Haltung der Umfrageteilnehmer hinsichtlich der Verschärfung der Datenschutzregeln für Behörden und Forschung nicht vom Beschäftigungssektor abhängig.

Von einer Zertifizierung und der Vergabe von Datenschutzlabels sind die Mitarbeitenden von grösseren Unternehmen/Organisationen eher angetan als jene von kleineren (250 oder mehr VZÄ: 62% Zustimmung; 0-9 VZÄ: 51% Zustimmung).

**Verbesserung der technischen Infrastruktur:** Hinsichtlich der technischen Infrastruktur besteht neben der Entwicklung von technischen Lösungen für die Sicherstellung des Datenschutzes (73% Zustimmung) in erster Linie im Bereich der Standardisierung kollektiver Handlungsbedarf. Aus Sicht von 69% der Befragten soll die Standardisierung von technischen Schnittstellen vorangetrieben werden, um es den verschiedenen Akteuren zu erlauben, die Chancen von Big Data besser wahrzunehmen. Des Weiteren sind 55% der Befragten der Ansicht, dass die Entwicklung von technischen Lösungen zur Verbesserung der Human-Data-Interaktion gefördert werden sollte (nur 15% sind hier gegenteiliger Meinung). Etwas verhaltener fällt das Votum aus, wenn es darum geht, die technische Infrastruktur für die Bereitstellung und Archivierung von sehr grossen Datenmengen bereitzustellen: Hier verorten 53% der Befragten kollektiven Handlungsbedarf, während 24% gegenteiliger Ansicht sind.

Die Verfügbarmachung der technischen Infrastruktur für die Bereitstellung und Archivierung von sehr grossen Datenmengen ist vor allem den Mitarbeitenden des öffentlichen Sektors (58% Zustimmung) ein Anliegen, während die Mitarbeitenden der Privatwirtschaft (43% Zustimmung) diesbezüglich keinen dringenden kollektiven Handlungsbedarf sehen.

**Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren:** 68% der Befragten sind der Ansicht, dass die rechtlichen Rahmenbedingungen für sichere Datenzentren verbessert werden sollten.

**Förderung von Open Data:** An erster Stelle wird hier die konsequente Umsetzung des Open-Data-Prinzips im Bereich der Forschung (66% Zustimmung) und in der öffentlichen Verwaltung (61%) genannt. 55% der Befragten sind zudem der Ansicht, dass das Open-Data-Prinzip generell auf alle Daten angewendet werden sollte, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen. Dies schliesst Daten aus dem privaten Sektor mit ein. 54% der Befragten erachten es als wichtig, dass die Sekundärnutzung von Daten in der Forschung speziell gefördert wird und 48% wünschen sich auch eine Förderung der Sekundärnutzung von Daten innerhalb der öffentlichen Verwaltung. Eher auf Ablehnung stösst hingegen die Förderung der Sekundärnutzung von Daten in der Privatwirtschaft (41% Ablehnung; 33% Zustimmung).

Die Forderung, dass das Open-Data-Prinzip mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen, angewendet werden soll, stösst bei den Mitarbeitenden der Privatwirtschaft (61% Zustimmung) auf grössere Begeisterung als bei jenen des öffentlichen Sektors (50% Zustimmung). Am höchsten ist die Zustimmungsrate bei den Mitarbeitenden von Kleinunternehmen (68% Zustimmung) und von Nonprofit-Organisationen (76%). Die Förderung der Sekundärnutzung von Daten innerhalb der öffentlichen Verwaltung wird von den

Mitarbeitenden des öffentlichen Sektors häufiger gewünscht (51% Zustimmung) als von den Mitarbeitenden der Privatwirtschaft (41% Zustimmung).

**Ausbildung von Datenspezialisten:** 64% der Befragten sind der Ansicht, dass die Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.) gefördert werden sollte.

**Verstärkung von Kontrollmechanismen:** Aus Sicht von 64% der Befragten ist die wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich zu verstärken. 53% erachten es zudem als notwendig, den Schutz von Whistleblowern zu verbessern und den investigativen Journalismus zu fördern. Eine Erweiterung der Kompetenzen für Datenschutzbeauftragte wünschen sich 50% der Befragten (wobei gut ein Viertel zusätzliche Kompetenzen für die Datenschützer nicht als notwendig erachten).

Der Schutz von Whistleblowern und die Förderung des investigativen Journalismus liegen den Mitarbeitenden der Privatwirtschaft (59% Zustimmung) weit stärker am Herzen als den Mitarbeitenden des öffentlichen Sektors (48% Zustimmung). Unter den Mitarbeitenden des öffentlichen Sektors ist die Zustimmungsrate umso höher, je grösser die Organisation ist, der jemand angehört: Während die Zustimmungsrate bei den Mitarbeitenden von grossen öffentlich-rechtlichen Organisationen 50% beträgt, beläuft sie sich bei jenen von kleinen Organisationen mit weniger als 50 VZÄ auf nur 38%. Kurioserweise ist der Grösseneffekt bei den Mitarbeitenden der Privatwirtschaft genau umgekehrt: Hier weisen die Mitarbeitenden von Kleinstunternehmen mit 71% die höchste Zustimmungsrate auf.

#### 7.7.2 Vernachlässigbare Handlungsfelder

Ob hinsichtlich der Forschung im Bereich der künstlichen Intelligenz kollektiver Handlungsbedarf besteht, ist umstritten: 41% der Befragten stimmen zu; 30% sind gegenteiliger Meinung.

### 7.8 Zuständigkeit und Koordinationsbedarf

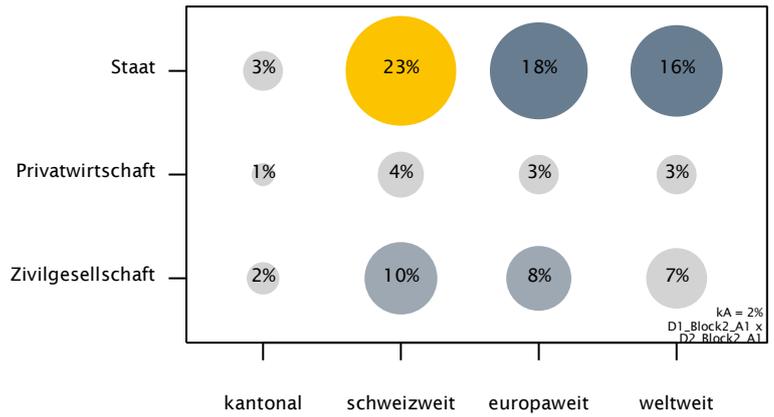
Neben der Identifikation von Bereichen mit kollektivem Handlungsbedarf wurden die Umfrageteilnehmer auch gebeten anzugeben, ob sie am ehesten den Staat, die Privatwirtschaft oder die Zivilgesellschaft bei der Umsetzung der Massnahmen in der Pflicht sehen und auf welcher Ebene die intendierten Massnahmen koordiniert werden sollen (kantonal/regional, schweizweit, europaweit oder weltweit). Der Übersichtlichkeit halber werden hier nur jene Massnahmen behandelt, die entweder von mindestens 60% aller Befragten oder von mindestens 60% der in der Privatwirtschaft tätigen Befragten befürwortet werden (die Details zu den übrigen Massnahmen sind im Anhang 5 zu finden). Die Massnahmen sind zudem gemäss den staatlichen Handlungsfeldern angeordnet (in Anlehnung an Tabelle 2). Wir haben auch hier die Ergebnisse darauf hin überprüft, inwieweit die in der Privatwirtschaft tätigen Befragten in ihren Einschätzungen von jenen der im öffentlichen Sektor Beschäftigten abweichen; dabei konnten keine statistisch signifikanten Unterschiede festgestellt werden.

#### 7.8.1 Regulatorische Massnahmen

Bei den regulatorischen Massnahmen ist in erster Linie der Staat gefordert (siehe Abbildung 22). In drei von vier Fällen kann die Koordination auf nationaler Ebene erfolgen. Dazu gehören die Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten, die Verschärfung der Datenschutzregeln für die Privatwirtschaft sowie die Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren. In allen drei Fällen ist jedoch eine Abstimmung auf internationaler Ebene wünschenswert. Bei der Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten ist zudem auch die Zivilgesellschaft gefordert, während bei der Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren auch die Privatwirtschaft mit einbezogen werden sollte. Hinsichtlich der verstärkten wettbewerbsrechtlichen Kontrolle von (Quasi-)Monopolisten im Internet-Bereich ist neben einer schweizweiten auch eine weltweite Koordination vonnöten; eine europaweite Abstimmung wäre ebenfalls hilfreich.

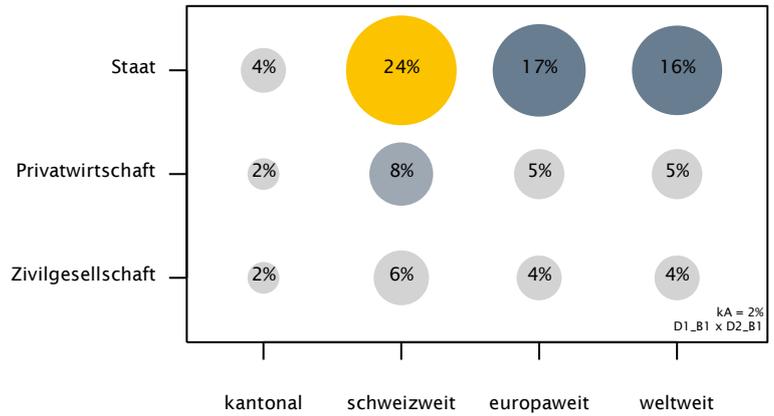
**Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten**

Zustimmungsrate: 75.1% (N = 604)  
 Neutrale: 14.8% (N = 119)  
 Ablehnungsrate: 10.1% (N = 81)



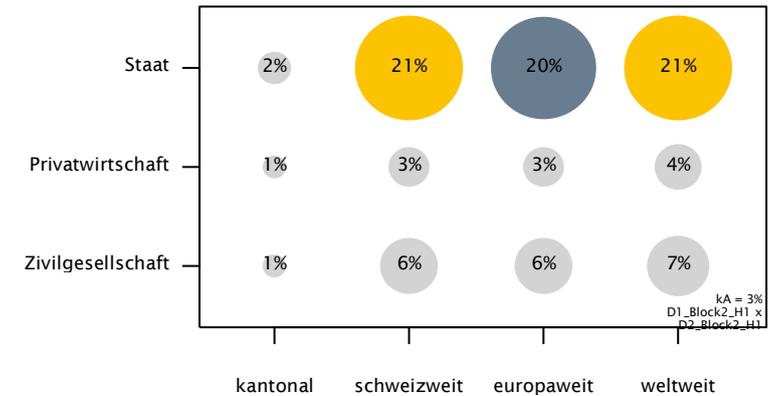
**Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren**

Zustimmungsrate: 68.5% (N = 539)  
 Neutrale: 21.2% (N = 167)  
 Ablehnungsrate: 10.3% (N = 81)



**Verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-) Monopolisten im Internet-Bereich**

Zustimmungsrate: 63.9% (N = 507)  
 Neutrale: 22.4% (N = 178)  
 Ablehnungsrate: 13.6% (N = 108)



**Verschärfung der Datenschutzregeln für die Privatwirtschaft**

Zustimmungsrate: 61.1% (N = 490)  
 Neutrale: 20.4% (N = 164)  
 Ablehnungsrate: 18.5% (N = 148)

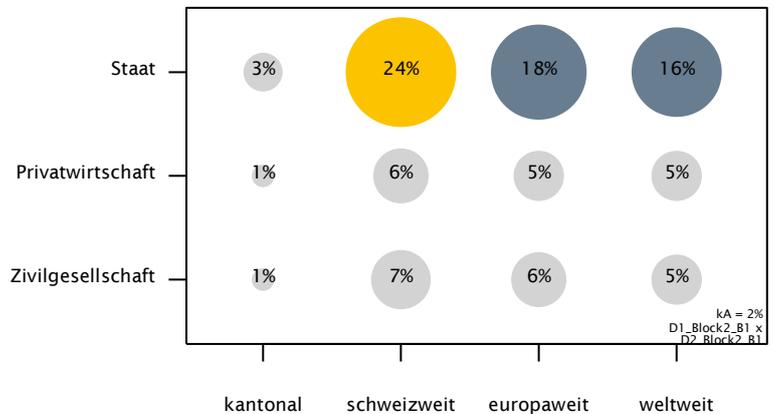


Abbildung 22: Zuständigkeit und Koordinationsbedarf bei den regulatorischen Massnahmen

## 7.8.2 Standardisierungsaufgaben

Im Hinblick auf die Standardisierung von technischen Schnittstellen ist in erster Linie die Privatwirtschaft gefragt, wobei die Koordination weltweit erfolgen sollte. Das schliesst aber eine Koordination auf europäischer bzw. nationaler Ebene nicht aus; auch diese wird von den Befragten als wichtig erachtet. Neben der Privatwirtschaft hat auch der Staat einen Beitrag zur Standardisierung zu leisten.

### Standardisierung von technischen Schnittstellen

Zustimmungsrate: 69.1% (N = 542)

Neutrale: 22.3% (N = 175)

Ablehnungsrate: 8.5% (N = 67)

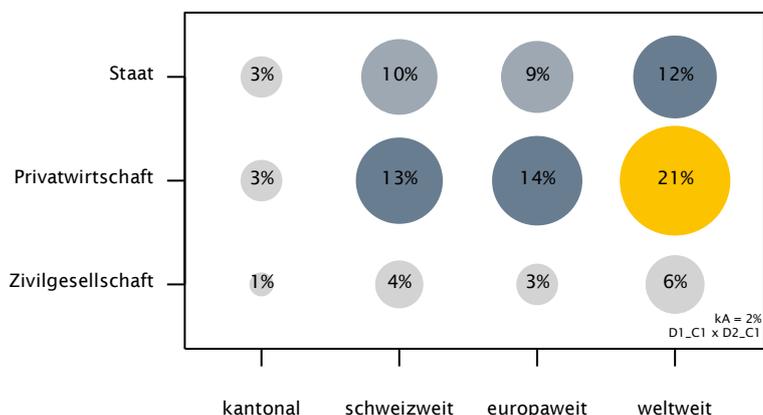


Abbildung 23: Zuständigkeit und Koordinationsbedarf bei den Standardisierungsaufgaben

## 7.8.3 Flankierende Massnahmen

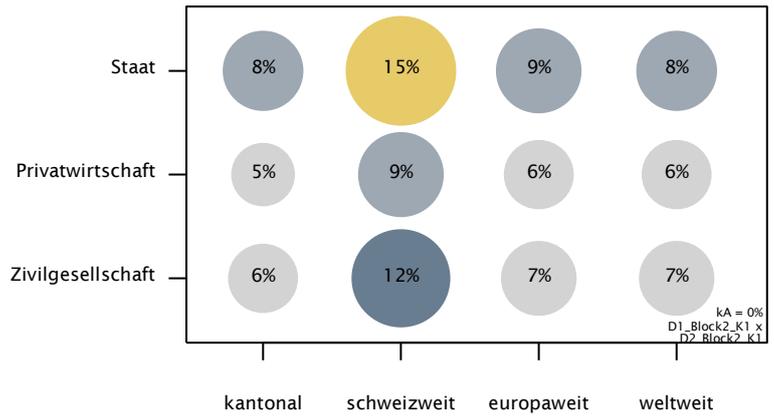
Bei den flankierenden Massnahmen zeigt sich ein durchzogenes Bild: Hier sind sowohl der Staat als auch die Privatwirtschaft gefragt, wobei die Koordination in erster Linie auf nationaler Ebene erfolgen sollte. Bei den Aufklärungs- und Sensibilisierungsmassnahmen sehen die Befragten am ehesten den Staat in der Lead-Rolle, wobei der Zivilgesellschaft und der Privatwirtschaft ebenfalls eine wichtige Rolle zukommt. Die Aktivitäten sollten zudem mit den Kantonen wie auch auf internationaler Ebene koordiniert werden.

Im Hinblick auf das Schaffen von Mechanismen, welche es den Einzelnen erlauben, ihre personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben, sehen die Befragten am ehesten den Staat in der Lead-Rolle, wobei der Privatwirtschaft und den zivilgesellschaftlichen Akteuren ebenfalls eine wichtige Rolle zukommt. Zudem sollten die Aktivitäten in diesem Bereich nicht nur auf nationaler Ebene, sondern auch europaweit koordiniert werden. Eine paritätisch geteilte Verantwortung zwischen Staat und Privatwirtschaft sehen die Befragten, wenn es darum geht, Dienste bereitzustellen, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen. Auch hier kommt der Zivilgesellschaft eine wichtige Rolle zu. Zudem wird der internationalen Koordination der Aktivitäten neben der nationalen Koordination eine recht grosse Bedeutung zugemessen.

Die Aus- und Weiterbildung von Datenspezialisten sollte aus Sicht der Befragten vor allem von der Privatwirtschaft gefördert werden, wobei dem Staat eine wichtige Rolle zukommt und sich auch die zivilgesellschaftlichen Akteure einbringen sollten. Hier halten die Befragten neben der nationalen Koordination eine Koordination auf europäischer Ebene für sinnvoll. Ähnlich steht es mit der Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes: Auch hier sehen die Befragten die Führungsrolle bei der Privatwirtschaft, wobei dem Staat wiederum eine wichtige Rolle zukommt. Die Koordination sollte hier aus Sicht der Befragten nicht nur national und europaweit, sondern auch weltweit stattfinden.

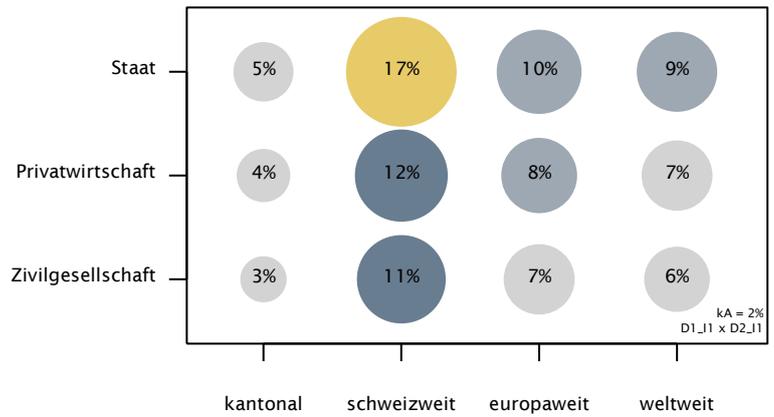
### Aufklärungs- und Sensibilisierungsmassnahmen

Zustimmungsrate: 71.9% (N = 581)  
 Neutrale: 20.4% (N = 165)  
 Ablehnungsrate: 7.7% (N = 62)



### Schaffen von Mechanismen, welche es dem Einzelnen erlauben, seine personen-bezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben (z.B. im Gesundheitsbereich)

Zustimmungsrate: 67.5% (N = 545)  
 Neutrale: 18.5% (N = 149)  
 Ablehnungsrate: 14% (N = 113)



### Bereitstellung von Diensten, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen

Zustimmungsrate: 67.2% (N = 526)  
 Neutrale: 20.9% (N = 164)  
 Ablehnungsrate: 11.9% (N = 93)

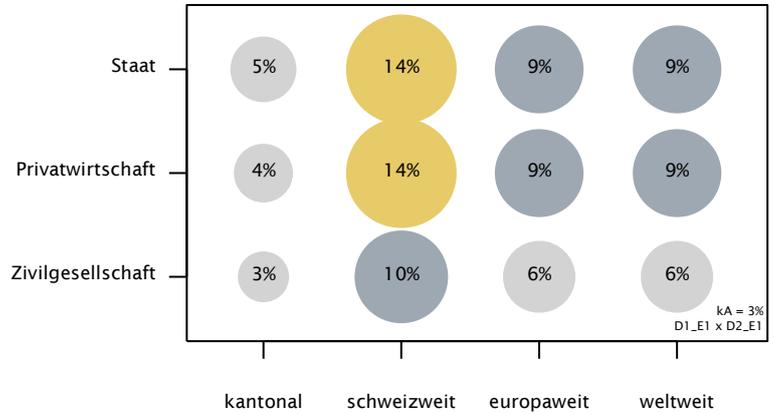
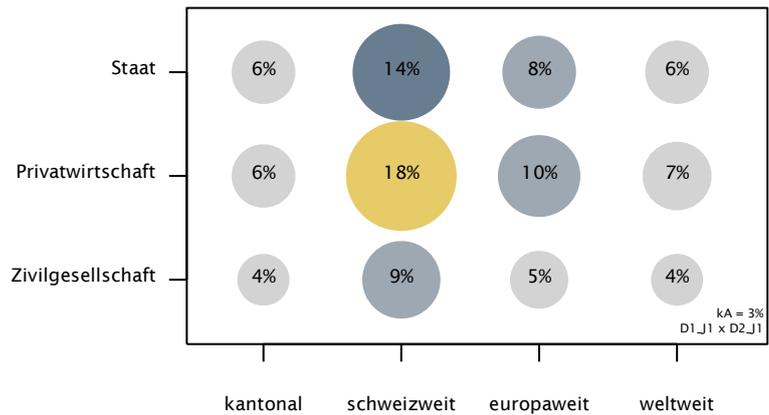


Abbildung 24a: Zuständigkeit und Koordinationsbedarf bei den flankierenden Massnahmen

**Förderung der Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.)**

Zustimmungsrate: 64.2% (N = 512)  
 Neutrale: 22.8% (N = 182)  
 Ablehnungsrate: 12.9% (N = 103)



**Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes**

Zustimmung: 73.1% (N = 591)  
 Neutrale: 17.9% (N = 145)  
 Ablehnung: 8.9% (N = 72)

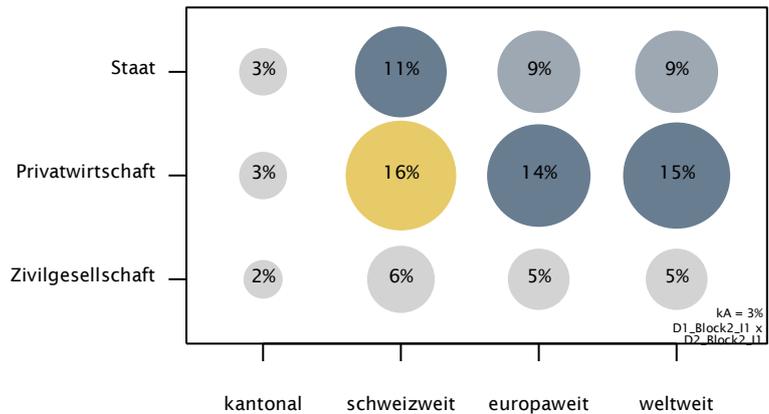


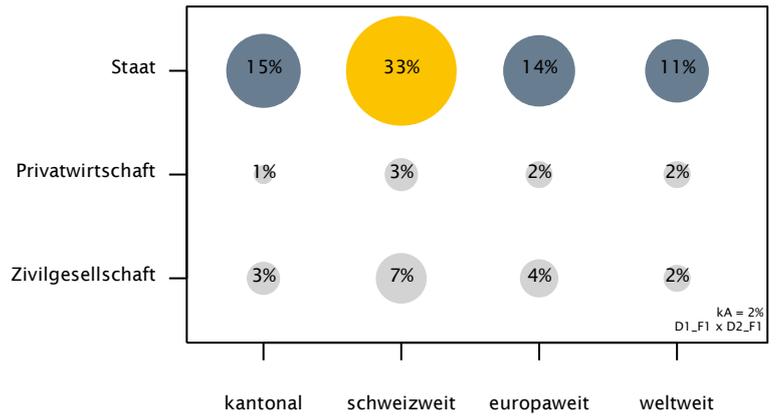
Abbildung 24b: Zuständigkeit und Koordinationsbedarf bei den flankierenden Massnahmen (Fortsetzung)

7.8.4 Verwaltungstätigkeit / Forschungstätigkeit

Im Hinblick auf die konsequente Umsetzung des Open-Data-Prinzips in diversen Bereichen sehen die Befragten vor allem den Staat in der Pflicht, wobei die Koordination wiederum vor allem auf nationaler Ebene erfolgen sollte. Bezüglich der Öffnung der eigentlichen Verwaltungsdaten liegt der Ball bei der öffentlichen Verwaltung selber. Hier sollten die Anstrengungen aus Sicht der Befragten primär auf nationaler Ebene koordiniert werden, wobei der Koordination auf kantonaler und auf internationaler Ebene ebenfalls eine wichtige Bedeutung zugemessen wird. Im Hinblick auf die Öffnung von Forschungsdaten ist neben den staatlichen Akteuren auch die Privatwirtschaft gefragt; hier sollte die Koordination neben der nationalen Ebene verstärkt auch auf internationaler Ebene stattfinden. Bei der Öffnung der Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen, wird die Federführung am ehesten beim Staat gesehen, wobei die Aktivitäten neben der nationalen Ebene auch auf kantonaler und europäischer Ebene koordiniert werden sollten. Auch der Zivilgesellschaft wird hier eine wichtige Rolle eingeräumt.

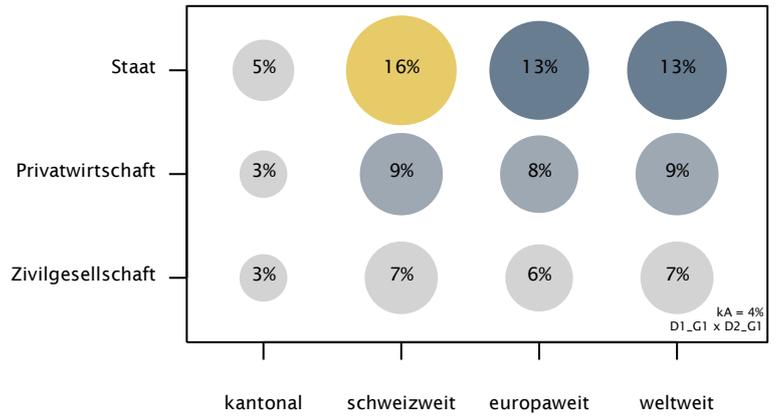
**Konsequente Umsetzung des Open-Data-Prinzips in der öffentlichen Verwaltung**

Zustimmungsrate: 61.4% (N = 486)  
 Neutrale: 22.9% (N = 181)  
 Ablehnungsrate: 15.8% (N = 125)



**Konsequente Umsetzung des Open-Data-Prinzips im Bereich der Forschung**

Zustimmungsrate: 66.1% (N = 516)  
 Neutrale: 19.6% (N = 153)  
 Ablehnungsrate: 14.3% (N = 112)



**Konsequente Umsetzung des Open Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor)**

Zustimmungsrate: 55.5% (N = 435)  
 Neutrale: 24.4% (N = 191)  
 Ablehnungsrate: 20.2% (N = 158)

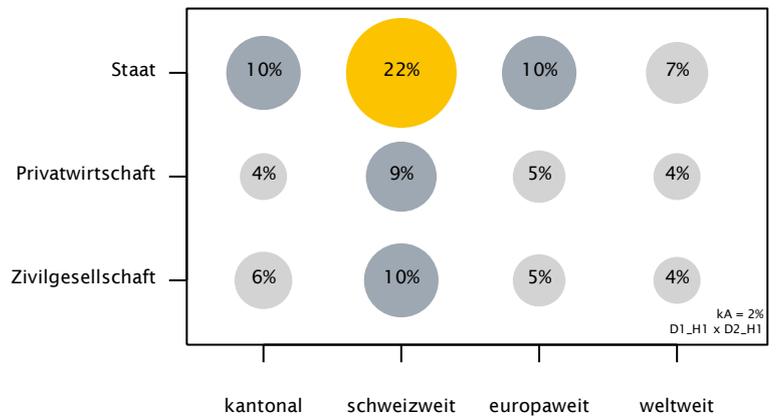


Abbildung 25: Zuständigkeit und Koordinationsbedarf bezüglich der Verwaltungs- bzw. Forschungstätigkeit

## 7.9 Handlungsprioritäten der verschiedenen Akteure

Anhand der Priorisierung der Massnahmen und der Einschätzung, durch wen die Massnahme am ehesten angegangen werden soll, lässt sich für die verschiedenen Akteure mit Blick auf die Förderung der Chancen bzw. die Verminderung der Risiken von Big Data Handlungsprioritäten ableiten. Diese sind nachfolgend in tabellarischer Form aufgeführt.

### 7.9.1 Handlungsprioritäten Bund

Tabelle 7 gibt einen Überblick über die Handlungsprioritäten des Bundes. Bei der Kontrolle von (Quasi-)Monopolisten im Internet-Bereich ist zu beachten, dass diese im internationalen Kontext angegangen werden sollte. Die Massnahmen, welche in enger Abstimmung mit der Privatwirtschaft umgesetzt werden sollten, sind im nächsten Abschnitt aufgeführt.

Zustimmungsrate	Lead	Massnahme
75%	Bund	Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten
72%	Bund	Aufklärungs- und Sensibilisierungsmassnahmen
68%	Bund	Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren
64%	Bund / international	Verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich
61%	Bund	Verschärfung der Datenschutzregeln für die Privatwirtschaft
61%	Bund	Konsequente Umsetzung des Open-Data-Prinzips in der öffentlichen Verwaltung
55% (Beschäftigte privater Sektor: 61%)	Bund	Konsequente Umsetzung des Open-Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor)

Tabelle 7: Handlungsprioritäten Bund

## 7.9.2 Handlungsprioritäten Bund in Kooperation mit der Privatwirtschaft

Tabelle 8 gibt einen Überblick über die Handlungsprioritäten des Bundes in Kooperation mit der Schweizer Privatwirtschaft. Bei der Standardisierung von technischen Schnittstellen ist zu beachten, dass diese vor allem auf weltweiter Ebene koordiniert werden sollte. Als „Lead“ ist derjenige Akteur aufgeführt, dem von den meisten Befragten die Verantwortung für die Massnahme zugeschrieben wird.

Zustimmungsrate	Lead	Massnahme
73%	Private	Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes
69%	Private (international)	Standardisierung von technischen Schnittstellen
68%	Bund	Schaffen von Mechanismen, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben
67%	Bund / Private	Bereitstellung von Diensten, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen
66%	Bund	Konsequente Umsetzung des Open-Data-Prinzips im Bereich der Forschung
64%	Private	Förderung der Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.)

Tabelle 8: Handlungsprioritäten Bund und Schweizer Privatwirtschaft

### 7.9.3 Rolle der Zivilgesellschaft

Tabelle 9 gibt einen Überblick über die Massnahmen, bei denen die Zivilgesellschaft aus Sicht der Befragten einen substantiellen Beitrag leisten sollte. Dabei wird die Anzahl Nennungen aufgeführt, mit denen die zivilgesellschaftlichen Akteure der Schweiz bei der Festlegung der Zuständigkeit für die jeweilige Massnahme bedacht wurden. Aufgeführt werden alle Massnahmen, die mindestens 100 Nennungen aufweisen. Man beachte, dass die Tabelle daher auch Massnahmen enthält, denen weniger als 60% der Befragten zustimmen.

Anzahl Nennungen	Zustimmungsrate	Massnahme
325	72%	Aufklärungs- und Sensibilisierungsmassnahmen
214	68%	Schaffen von Mechanismen, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben
174	75%	Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten
168	67%	Bereitstellung von Diensten, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen
161	64%	Förderung der Aus- und Weiterbildung von Datenspezialisten
140	53%	Verbesserung des Schutzes von Whistleblowern / Förderung des investigativen Journalismus
135	55% (Beschäftigte priv. Sektor: 61%)	Konsequente Umsetzung des Open Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen
120	73%	Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes
116	61%	Konsequente Umsetzung des Open Data-Prinzips im Bereich der Forschung
112	58%	Vergabe von Datenschutzlabels im Rahmen einer Zertifizierung von Unternehmen/Organisationen
106	56%	Zertifizierung von Unternehmen und Vergabe von Datenschutzlabels zur Durchsetzung höherer Datenschutzstandards am Markt

Tabelle 9: Rolle der Zivilgesellschaft

## 7.10 Die Perspektiven verschiedener Stakeholder-Gruppen im Vergleich

Um die Perspektiven verschiedener Stakeholder-Gruppen besser herauszuarbeiten und um aufzuzeigen, in welchen Fragen die in der Stichprobe untervertretenen Gruppen von der Mehrheit abweichen, wurde eine Reihe von Vergleichsanalysen angestellt.<sup>8</sup>

### 7.10.1 Unterschiede hinsichtlich Geschlecht, Alter, Sprache, Wohn- und Arbeitsort

Da Frauen in der Stichprobe stark untervertreten sind, interessieren zunächst einmal die Geschlechterunterschiede: Der einzige signifikante Unterschied, der identifiziert werden konnte, betrifft die Einschätzung der Chancen und Risiken von Big Data aus persönlicher Sicht. Während 52% der befragten Männer der Ansicht sind, dass die Chancen von Big Data aus ihrer persönlichen Sicht überwiegen, teilen nur 40% der Frauen diese Auffassung. Dieser Unterschied besteht auch, wenn man die Männer und Frauen miteinander vergleicht, die im Bereich „Technik, Informatik“ tätig sind. Wenn es hingegen darum geht, die Chancen und Risiken von Big Data aus Sicht des Arbeitgebers zu beurteilen, entfällt der Geschlechterunterschied. Bei den Fragen hinsichtlich der Auswirkungen von Big Data, der Grundsätze der Data Governance und des kollektiven Handlungsbedarfs sind keine nennenswerten Geschlechterunterschiede zu verzeichnen.

Was die Unterschiede zwischen den verschiedenen Altersgruppen betrifft, so können aufgrund der geringen Stichprobengrösse kaum Aussagen über die Personen unter 30 Jahren und jene über 70 Jahren gemacht werden. Dies stellt insofern ein Problem dar, als einige der festgestellten Unterschiede zwischen den Altersgruppen nicht linear verlaufen. So assoziiert beispielsweise die Gruppe der 40 bis 49-Jährigen Big Data eher mit zunehmenden Möglichkeiten der Personalisierung als die Gruppe der über 60-Jährigen (61% vs. 50%); eine Tendenz, dass jüngere Menschen diesen Aspekt generell höher einschätzen als ältere, lässt sich aus den Daten jedoch nicht ablesen. Anders ist es bei der Einschätzung der Bedrohung der Privatsphäre. Hier wird die Gefahr mit zunehmendem Alter höher eingeschätzt.<sup>9</sup> Bezüglich der Einschätzung der übrigen Auswirkungen von Big Data (Höhe der Auswirkungen; zunehmende Gefahr der Manipulation; zunehmende Optimierungsmöglichkeiten) konnten keine Altersunterschiede festgestellt werden. Was die Grundlagen der Data Governance anbelangt, so sind ältere Umfrageteilnehmer eher der Ansicht, dass Personendaten unbedingt geschützt werden müssen und ihre Preisgabe problematisch sein kann, als jüngere.<sup>10</sup> Ein Alterseffekt ist auch bei der Einschätzung festzustellen, ob die Leute für die Preisgabe ihrer Daten eine faire Gegenleistung erhalten; hier sind die älteren Umfrageteilnehmer kritischer eingestellt als die jüngeren.<sup>11</sup> Bezüglich der übrigen Grundlagen der Data Governance (Notwendigkeit staatlicher Eingriffe auf dem Datenmarkt; Sicherstellung des Datenschutzes durch ein Empowerment der Nutzer; relativistische Ansätze bezüglich Datenschutz) konnten keine signifikanten Altersunterschiede festgestellt werden. Was den kollektiven Handlungsbedarf betrifft, so verorten die über 60-Jährigen und die unter 40-Jährigen tendenziell in mehr Bereichen Bedarf an Massnahmen als die 40 bis 49-Jährigen.<sup>12</sup> Was die konkreten Massnahmen anbelangt, so fordern die unter 40-Jährigen häufiger eine konsequente Umsetzung des Open-Data-Prinzips als die älteren Befragten (81% vs. 68%). Ebenso fordern sie häufiger eine Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) als die älteren Befragten, wobei hier der Zusam-

<sup>8</sup> Hierzu wurden bei den Fragen der Abschnitte B und C des Fragebogens anhand von Hauptkomponentenanalysen die verschiedenen Dimensionen eruiert und die dazugehörigen Werte (scores) ermittelt (siehe Anhang 6). Anschliessend wurden diverse Kreuztabellen erstellt, um die Zusammenhänge zwischen den einzelnen Variablen zu untersuchen.

<sup>9</sup> Bedrohung der Privatsphäre – unter 40 Jahre: 78%; 40-49 Jahre: 79%; 50-59 Jahre: 83%; über 60 Jahre: 88%.

<sup>10</sup> Personendaten müssen unbedingt geschützt werden; die Preisgabe kann problematisch sein – unter 40 Jahre: 80%; 40-49 Jahre: 84%; 50-59 Jahre: 88%; über 60 Jahre: 93%.

<sup>11</sup> Faire Gegenleistung – unter 40 Jahre: 15%; 40-49 Jahre: 9%; 50-59 Jahre: 7%; über 60 Jahre: 3%.

<sup>12</sup> Anteil der Personen, die in über 15 Bereichen kollektiven Handlungsbedarf verorten – unter 40 Jahre: 45%; 40-49 Jahre: 34%; 50-59 Jahre: 39%; über 60 Jahre: 47%.

menhang mit dem Alter nicht linear ist.<sup>13</sup> Für eine Verschärfung der Datenschutzregeln sprechen sich eher die älteren Befragten aus, wobei auch hier der Zusammenhang mit dem Alter nicht linear ist.<sup>14</sup> Einen klaren, wenn auch nicht sehr ausgeprägten Zusammenhang mit dem Alter lässt sich hingegen hinsichtlich der Notwendigkeit von Massnahmen für ein Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten feststellen: je älter die Befragten, desto höher die Zustimmungsrates.<sup>15</sup> Hinsichtlich der übrigen Massnahmenbereiche (Förderung der Sekundärnutzung von Daten; Einführung von Datenschutzlabels, Verbesserung der rechtlichen Rahmenbedingungen für Datenzentren; Standardisierung von technischen Schnittstellen) lassen sich keine Alterseffekte feststellen.

Regionale Unterschiede gibt es etliche, wobei die Grenzen jeweils unterschiedlich verlaufen. In mehreren Fällen lässt sich ein Unterschied zwischen der Westschweiz und der Deutschschweiz feststellen, der sich auch als Unterschied zwischen Sprachgruppen manifestiert, wobei auch hier die Unterschiede zwischen den einzelnen Regionen der Deutschschweiz und der Westschweiz bisweilen recht ausgeprägt sein können, so dass übers Ganze gesehen nicht von einem „Röschtigraben“ die Rede sein kann. In den folgenden Bereichen scheinen die Sensibilitäten der Französischsprachigen etwas anders ausgeprägt zu sein als jene der Deutschsprachigen: Aus Sicht der Französischsprachigen hat Big Data stärkere Auswirkungen – 41% der Französischsprachigen schätzen das Potential von Big Data als hoch oder sehr hoch ein, gegenüber 25% der Deutschsprachigen. Konkret zeigt sich dies insbesondere bei der Beurteilung der Auswirkungen im Bereich der Personalisierung (71% der Französischsprachigen rechnen hier mit bedeutenden Auswirkungen, während es bei den Deutschsprachigen nur 54% sind). Zudem schätzen die Französischsprachigen die Bedrohung der Privatsphäre durch Big Data eher als hoch ein als die Deutschsprachigen; der Unterschied ist aber nicht sehr ausgeprägt (88% vs. 80%). Hinsichtlich der Grundlagen der Data Governance besteht ein wichtiger Unterschied zwischen Romands und Deutschschweizern darin, dass die ersteren eher zur Ansicht neigen, der Staat müsse auf dem Datenmarkt regulierend eingreifen (90% vs. 78%). Zudem neigen die Französischsprachigen weniger häufig zur Ansicht, dass eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten nicht sinnvoll ist (31% vs. 47%). Was den kollektiven Handlungsbedarf anbelangt, so verorten die Romands tendenziell in mehr Bereichen Handlungsbedarf als die Deutschschweizer. Dies gilt insbesondere für die Stärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) (81% vs. 63%), für die Verschärfung der Datenschutzregeln (66% vs. 50%) und für die Forderung nach Datenschutzlabels (86% vs. 70%). Zudem sehen die Romands die Privatwirtschaft bei der Umsetzung der einzelnen Massnahmen etwas weniger häufig in der Pflicht als die Deutschschweizer (29% vs. 39%).

#### 7.10.2 Unterschiede hinsichtlich des persönlichen Bezugs zu Daten

Ob jemand oft beruflich mit Daten zu tun hat oder ob er sich im Rahmen des politischen oder zivilgesellschaftlichen Engagements für datenbezogene Belange einsetzt, hat keinen Einfluss auf die Einschätzung der Auswirkungen von Big Data. Anders ist es bei den Personen, die sich in ihrem Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinandersetzen, wobei die intensivere Auseinandersetzung mit den Fragen der Datennutzung durchaus auch das Ergebnis einer höheren Sensibilität gegenüber den Auswirkungen von Big Data sein kann. Personen, bei denen diese persönliche Betroffenheit gegeben ist, schätzen die Auswirkungen von Big Data höher ein: 39% bewerten das Potential von Big Data als hoch oder sehr hoch, gegenüber 20% bei den übrigen Befragten. So gehen sie eher davon aus, dass Big Data eine erhöhte Gefahr der Manipulation nach sich zieht (75% vs. 60%), neue Möglichkeiten zur Personalisierung von Angeboten, Preisen, usw. eröffnet (66% vs. 51%) und eine Bedrohung für die Privatsphäre darstellt (88% vs. 77%). Interessanterweise schätzen sie

<sup>13</sup> Es braucht eine Verstärkung von Kontrollmechanismen: unter 40 Jahre: 73%; 40-49 Jahre: 61%; 50-59 Jahre: 68%; über 60 Jahre: 68%.

<sup>14</sup> Es braucht eine Verschärfung der Datenschutzregeln: unter 40 Jahre: 55%; 40-49 Jahre: 47%; 50-59 Jahre: 53%; über 60 Jahre: 66%.

<sup>15</sup> Es braucht ein Empowerment der Nutzer: unter 40 Jahre: 85%; 40-49 Jahre: 87%; 50-59 Jahre: 88%; über 60 Jahre: 94%.

aber die relative Bedeutung der Chancen und Risiken von Big Data ähnlich ein wie die übrigen Befragten.

Was die Grundlagen der Data Governance anbelangt, tendieren jene Befragten, die beruflich nicht mit Daten zu tun haben, eher dazu, mit Blick auf die Kontrolle der personenbezogenen Daten ein Empowerment der Nutzer zu fordern (100% vs. 90%). Dasselbe gilt für die Befragten, die sich im Bereich der Daten politisch oder zivilgesellschaftlich engagieren (94% vs. 89%) und für jene, die sich im Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinandersetzen (94% vs. 88%). Letztere neigen auch eher zur Ansicht, der Staat müsse auf dem Datenmarkt regulierend eingreifen (85% vs. 77%). Ansonsten hat die Art des Bezugs zu Daten keinen Einfluss auf die Haltung der Befragten bezüglich der verschiedenen Aspekte der Data Governance.

Was den kollektiven Handlungsbedarf anbelangt, so sehen jene Personen, die sich im Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinandersetzen, in mehr Bereichen einen Bedarf an Massnahmen als die übrigen. Dies betrifft eine ganze Palette von Handlungsbereichen, wie die Stärkung der Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) (77% vs. 59%), die Verschärfung der Datenschutzregeln (59% vs. 49%), die konsequente Umsetzung des Open-Data-Prinzips (76% vs. 66%), das Empowerment der Nutzer (93% vs. 84%) sowie die Einführung von Datenschutzlabels (76% vs. 70%). Ob sich jemand politisch oder zivilgesellschaftlich für datenbezogene Belange einsetzt oder nicht, hat kaum einen Einfluss auf die Einschätzung des kollektiven Handlungsbedarfs, mit Ausnahme der konsequenten Umsetzung des Open-Data-Prinzips (77% vs. 66%). Ebenso wenig spielt es eine Rolle, ob jemand oft im Beruf mit Daten zu tun hat oder nicht. Hier bildet die Forderung nach besseren Kontrollmechanismen die einzige Ausnahme: Befragte, welche oft beruflich mit Daten zu tun haben, fordern seltener bessere Kontrollmechanismen als die übrigen (62% vs. 82%). Generell scheinen demnach die Haltungen der Befragten bezüglich Big Data weit stärker mit einem Gefühl der persönlichen Betroffenheit zusammenzuhängen, als mit der beruflichen Exponiertheit oder einem politischen oder zivilgesellschaftlichen Engagement.

Dies trifft auch weitgehend zu, wenn man zusätzlich betrachtet, inwiefern die Haltungen der Befragten variieren, je nachdem in welchem Ausmass ihr Arbeitgeber Big Data einsetzt (gemessen auf einer Skala von 0 bis 3 „V“ – für „Volume“, „Velocity“ und „Variety“). Hier fällt jedoch auf, dass Beschäftigte von Unternehmen und Organisationen, in denen die 3 „V“ präsent sind, eher zur Ansicht neigen, der Staat müsse auf dem Datenmarkt regulierend eingreifen.<sup>16</sup> Dem entspricht auch, dass Beschäftigte von Unternehmen mit Big Data (3 „V“) in mehr Bereichen Massnahmen fordern als die übrigen, wobei der Unterschied hauptsächlich darin besteht, dass sie viel stärker dazu neigen, Massnahmen zur Förderung der Sekundärnutzung von Daten zu fordern als die übrigen.<sup>17</sup> Auch bringen sie Big Data eher mit der Optimierung von Prozessen in Verbindung<sup>18</sup> und bewerten die Chancen von Big Data aus persönlicher Sicht höher als die übrigen Befragten<sup>19</sup>.

### 7.10.3 Unterschiede hinsichtlich des Beschäftigungssektors, der Organisationsgrösse und der Branche

Im Vergleich mit jenen des öffentlichen Sektors neigen die Beschäftigten der Privatwirtschaft eher dazu, die Chancen von Big Data höher einzuschätzen als die Risiken. Dies gilt sowohl für ihre persönliche Sicht (55% vs. 46%) als auch für die Beurteilung aus Sicht ihres Arbeitgebers (72% vs. 60%). Allerdings schätzen sie die Auswirkungen von Big Data in allen Bereichen praktisch gleich ein wie die Beschäftigten des öffentlichen Sektors, mit Ausnahme der zunehmenden Personalisierung (65% vs. 54%). Was die Haltungen gegenüber den verschiedenen Aspekten der Data Governance betrifft, so ist festzustellen, dass die Beschäftigten des öffentlichen Sektors eher zur Ansicht neigen, der Staat müsse auf dem Datenmarkt regulierend eingreifen (84% vs. 75%), während die Beschäftigten der Privatwirtschaft vermehrt auf ein Empowerment der Nutzer setzen (93% vs. 88%) und eher davon

<sup>16</sup> Der Staat muss regulierend eingreifen: 0 „V“: 77%; 1 „V“: 78%; 2 „V“: 79%; 3 „V“: 86%.

<sup>17</sup> Massnahmen zur Förderung der Sekundärnutzung von Daten sind nötig: 0 „V“: 59%; 1 „V“: 54%; 2 „V“: 60%; 3 „V“: 70%.

<sup>18</sup> Big Data führt zu einer Optimierung von Prozessen: 0 „V“: 77%; 1 „V“: 80%; 2 „V“: 78%; 3 „V“: 87%.

<sup>19</sup> Aus persönlicher Sicht überwiegen die Chancen von Big Data über die Risiken: 0 „V“: 46%; 1 „V“: 35%; 2 „V“: 50%; 3 „V“: 57%.

ausgehen, dass diese für die Preisgabe ihrer Daten eine faire Gegenleistung erhalten (12% vs. 7%). Die Unterschiede sind jedoch gering. Keine signifikanten Unterschiede ergeben sich überdies, wenn man die verschiedenen Massnahmenbereiche gruppiert betrachtet; auf die Unterschiede bei den einzelnen Massnahmen wurde bereits in Kapitel 6.7 eingegangen.

Kaum ein signifikanter Zusammenhang besteht zwischen der Organisationsgrösse und den Haltungen der Befragten. Dies dürfte damit zusammenhängen, dass es sich bei den beobachteten Grösseneffekten oft nicht um lineare Zusammenhänge handelt und zudem zwischen den Sektoren Unterschiede bestehen. Ein positiver Grösseneffekt ist jedoch bezüglich der Einschätzung der Auswirkungen von Big Data im Bereich der Optimierung von Prozessen<sup>20</sup> und bei der Forderung nach der Einführung von Datenschutzlabels<sup>21</sup> festzustellen. Betrachtet man die Unternehmen der Privatwirtschaft separat, so sind noch ein paar weitere Grösseneffekte auszumachen: Die Einschätzung, dass Big Data zu einer Bedrohung der Privatsphäre führt, nimmt mit der Grösse des Unternehmens, für das jemand arbeitet, ab<sup>22</sup>, während die Chancen von Big Data aus persönlicher Sicht<sup>23</sup> und aus Sicht des Arbeitgebers<sup>24</sup> von den Angestellten von Grossunternehmen höher bewertet werden. Entsprechend sprechen sich Mitarbeitende von kleinen Unternehmen eher für ein Empowerment der Nutzer aus, als jene von Grossunternehmen.<sup>25</sup>

Neben dem Beschäftigungssektor und der Organisationsgrösse, hat auch die Branche, in der jemand tätig ist, einen Einfluss auf die Einschätzung verschiedener Big-Data-bezogener Aspekte: So befinden sich bei der Einschätzung, ob Big Data zu einer erhöhten Manipulationsgefahr führt, die im Gesundheits- oder Sozialwesen Beschäftigten und die Befragten aus dem Bereich „Unterrichtswesen, Forschung, Medien, Kultur“ mit Zustimmungsraten von 80% respektive 72% am oberen Ende der Skala, während die Bereiche „Management, Administration, Rechtswesen“ (62%), „andere Branchen“ (59%) und „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (57%) das untere Ende der Skala belegen. Bei der Einschätzung, ob Big Data zu vermehrten Prozessoptimierungsmöglichkeiten führt, liegen ebenfalls die Beschäftigten des Gesundheits- oder Sozialwesens mit 93% Zustimmung vorne, gefolgt von den Beschäftigten im Bereich „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ (90%), während die Beschäftigten der Bereiche „Management, Administration, Rechtswesen“ (80%), „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (78%) und „andere Branchen“ (71%) sich diesbezüglich weniger enthusiastisch äussern. Die Beschäftigten des Bereiches „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (70%) liegen jedoch vorne, was die Beurteilung der zusätzlichen Personalisierungsmöglichkeiten dank Big Data betrifft, während die Bereiche „Gesundheits und Sozialwesen“ (51%) und „Management, Administration, Rechtswesen“ (50%) das Schlusslicht bilden. Eine Bedrohung der Privatsphäre durch Big Data wird am stärksten von den Beschäftigten in den Bereichen „Unterrichtswesen, Forschung, Medien, Kultur“ (86%), „Management, Administration, Rechtswesen“ (84%) sowie „Technik, Informatik, Ingenieurwesen“ (81%) wahrgenommen, während die im Bereich „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ Tätigen diesen Aspekt mit einer Zustimmungsrate von 70% etwas weniger dramatisch einschätzen. Interessanterweise gibt es jedoch bei der Einschätzung des allgemeinen Potenzials von Big Data keine signifikanten Unterschiede zwischen den Branchen.

Kaum Unterschiede zwischen den Beschäftigten der einzelnen Branchen gibt es bei den Aspekten der Data Governance. Hier variiert einzig die Einschätzung, ob die Nutzer generell eine faire Gegen-

<sup>20</sup> Big Data führt zu einer Optimierung von Prozessen: 0-9 VZÄ: 77%; 10-49 VZÄ: 78%; 50-250 VZÄ: 80%; über 250 VZÄ: 85%.

<sup>21</sup> Datenschutzlabels sollten eingeführt werden: 0-9 VZÄ: 67%; 10-49 VZÄ: 66%; 50-250 VZÄ: 71%; über 250 VZÄ: 77%.

<sup>22</sup> Big Data führt zu einer Bedrohung der Privatsphäre: Privatwirtschaft, 0-9 VZÄ: 86%; 10-49 VZÄ: 78%; 50-250 VZÄ: 80%; über 250 VZÄ: 70%.

<sup>23</sup> Chancen von Big Data überwiegen aus persönlicher Sicht: Beschäftigte der Privatwirtschaft, 0-9 VZÄ: 48%; 10-49 VZÄ: 57%; 50-250 VZÄ: 49%; über 250 VZÄ: 68%.

<sup>24</sup> Chancen von Big Data überwiegen aus Sicht des Arbeitgebers: Beschäftigte der Privatwirtschaft, 0-9 VZÄ: 63%; 10-49 VZÄ: 70%; 50-250 VZÄ: 77%; über 250 VZÄ: 86%.

<sup>25</sup> Es braucht ein Empowerment der Nutzer: Beschäftigte der Privatwirtschaft, 0-9 VZÄ: 96%; 10-49 VZÄ: 94%; 50-250 VZÄ: 94%; über 250 VZÄ: 87%.

leistung für die Preisgabe ihrer Daten erhalten: Während die Befragten aus den Bereichen „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (16%), „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ (15%) noch am ehesten zur Ansicht neigen, das Austauschverhältnis sei fair, teilen die im Bereich „Management, Administration, Rechtswesen“ Tätigen (6%) diese Auffassung überhaupt nicht, wobei zu bemerken ist, dass die Unterschiede relativ gering sind und das Verdikt in allen Branchen sehr klar ausfällt.

Was den kollektiven Handlungsbedarf anbelangt, so gehören die Beschäftigten im Bereich „Unterrichtswesen, Forschung, Medien, Kultur“ zu denjenigen, die am meisten Massnahmen fordern, während sich die Beschäftigten in den Bereichen „Management, Administration, Rechtswesen“, „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ und „andere Branchen“ zurückhaltender zeigen. Dabei gewichten die Angehörigen der verschiedenen Branchen die Massnahmenbereiche unterschiedlich: Die Konsequente Umsetzung des Open-Data-Prinzips ist vor allem den Beschäftigten des Bereichs „Unterrichtswesen, Forschung, Medien, Kultur“ (78%) ein grosses Anliegen, während sie von den Beschäftigten der Bereiche „Technik, Informatik, Ingenieurwesen“ (67%) und „andere Branchen“ (62%) als weniger dringlich betrachtet wird. Demgegenüber sprechen sich die Vertreter des Bereichs „Transport, Verkehr, Telekommunikation, Energie- und Wasserversorgung“ (81%) am stärksten für Massnahmen zur Förderung der Sekundärnutzung von Daten aus, während sich die Beschäftigten der Bereiche „Unterrichtswesen, Forschung, Medien, Kultur“ (62%), „Technik, Informatik, Ingenieurwesen“ (61%) und „andere Branchen“ (46%) zurückhaltender zeigen. Bei der Forderung nach einer Verschärfung der Datenschutzregeln führen die Beschäftigten im Bereich „Sozial- und Gesundheitswesen“ (67%) das Feld an, während die Beschäftigten der Bereiche „Informationsdienstleistungen, Kommunikation, Werbung, Marketing“ (47%) und „Technik, Informatik, Ingenieurwesen“ (46%) diesbezüglich weniger starken Handlungsbedarf sehen. Für eine Stärkung der Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) sprechen sich am stärksten die Beschäftigten der Bereiche „Unterrichtswesen, Forschung, Medien, Kultur“ (79%) und „Sozial- und Gesundheitswesen“ (77%) aus, während die Befragten aus den Bereichen „Technik, Informatik, Ingenieurwesen“ (67%), „Management, Administration, Rechtswesen“ (60%) und „andere Branchen“ (56%) die geringsten Zustimmungsraten aufweisen. In ähnlicher Weise führen auch bei der Forderung nach einem Empowerment der Nutzer die Beschäftigten des Bereichs „Unterrichtswesen, Forschung, Medien, Kultur“ (95%) das Feld an, während die Beschäftigten in den Bereichen „Management, Administration, Rechtswesen“ (85%) und „Technik, Informatik, Ingenieurwesen“ (84%) etwas geringere Zustimmungsraten aufweisen. Praktisch umgekehrt verhält es sich hingegen bei der Forderung nach Massnahmen zur Standardisierung von technischen Schnittstellen: Hier liegen die Beschäftigten aus dem Bereich „Management, Administration, Rechtswesen“ (73%) vorne, während jene aus dem Bereich „Unterrichtswesen, Forschung, Medien, Kultur“ (63%) die geringste Zustimmungsraten aufweisen.

#### 7.10.4 Schlussfolgerungen hinsichtlich der Repräsentativität der Studie

Die vorangehenden Analysen erlauben es, ungefähr abzuschätzen, inwiefern eine hinsichtlich der schweizerischen Gesamtbevölkerung repräsentative Umfrage andere Ergebnisse liefern würde als die vorliegende Studie. Hierzu müssen die Unterschiede zwischen den Antworten jener Gruppen, die in der Stichprobe stark überrepräsentiert sind und jener, die stark unterrepräsentiert sind, analysiert werden. Stark überrepräsentiert sind in erster Linie Männer, Personen, welche beruflich mit Daten zu tun haben, Beschäftigte des öffentlichen Sektors sowie die Altersgruppe der 40 bis 59-Jährigen. Berücksichtigt werden in der folgenden Analyse Unterschiede von mehr als 10 Prozentpunkten, da die übrigen kaum ins Gewicht fallen (siehe Abbildung 26):

Hinsichtlich der Auswirkungen von Big Data ist zunächst die zunehmende Personalisierung zu nennen, welche von den Beschäftigten der Privatwirtschaft (unterrepräsentiert) tendenziell etwas höher bewertet wird. Im Falle einer repräsentativen Studie läge der Wert wohl rund 5 Prozentpunkte über dem eruierten Wert. Die Chancen von Big Data aus persönlicher Sicht werden von Männern (überrepräsentiert), von Beschäftigten der Privatwirtschaft (unterrepräsentiert) sowie von Beschäftigten von Betrieben mit Big Data (überrepräsentiert) höher bewertet. Die Unterschiede betragen je rund 10 Prozentpunkte und dürften sich in etwa neutralisieren.

	ist männlich	ist zwischen 40 und 59 Jahre alt	ist im öffentlichen Sektor beschäftigt	hat oft beruflich mit Daten zu tun	ist in einem Betrieb tätig, der Big Data (G-V) einsetzt	Wert (Stichprobe)	Korrigierter Wert (Grobe Schätzung)
Anteil in der Stichprobe	84%	69%	64%	95%	38%		
Anteil an der ständigen Wohnbevölkerung über 18 Jahre (BFS, 2014) bzw. an den in der Schweiz Beschäftigten (BFS, 2013)	49%	36%	13%	deutlich geringer	deutlich geringer		
<b>Auswirkungen von Big Data</b>							
Big Data hat ein grosses Potenzial						28%	n/a
Big Data erhöht die Gefahr von Manipulation						67%	n/a
Big Data ermöglicht die Optimierung von Abläufen und erhöht die Agilität					87% vs. 79%	82%	80%
Big Data ermöglicht die Personalisierung und die Identifikation von "schwarzen Schafen"			54% vs. 65%			58%	60-65%
Big Data bedroht die Privatsphäre und erhöht die Gefahr von Datendiebstahl, persönlicher Repression und Betrug						81%	n/a
Aus persönlicher Sicht überwiegen die Chancen von Big Data über die Risiken	52% vs. 40%		46% vs. 55%		57% vs. 45%	50%	45-55%
<b>Aspekte der Data-Governance</b>							
Der Staat muss intervenieren, weil der Datenmarkt nicht funktioniert.			84% vs. 75%		86% vs. 78%	81%	75-80%
Der Datenschutz ist durch ein Empowerment der Nutzer sicherzustellen.			88% vs. 93%	90% vs. 100%	88% vs. 92%	91%	95-100%
Personendaten müssen geschützt werden; ihre Preisgabe kann problematisch sein.						86%	n/a
Die Leute erhalten für die Preisgabe ihrer Daten eine faire Gegenleistung.			7% vs. 12%			9%	10%
Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt.					65% vs. 57%	60%	55-60%
Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten ist nicht sinnvoll.						45%	n/a
<b>Kollektiver Handlungsbedarf</b>							
Anzahl geforderter Massnahmen (Massnahmen in über 15 Handlungsfeldern)		36% vs. 46%			47% vs. 35%	39%	35-45%
Förderung der Sekundärnutzung von Daten					70% vs. 58%	62%	60%
Konsequente Umsetzung des Open-Data-Prinzips		68% vs. 75%				70%	70-75%
Verschärfung der Datenschutzregeln		50% vs. 60%				53%	55-60%
Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus)				66% vs. 82%		66%	70-80%
Datenschutzlabels, rechtliche Rahmenbedingungen für Datenzentren						72%	n/a
Standardisierung der technischen Schnittstellen						69%	n/a
Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten						88%	n/a

Abbildung 26: Analyse der Antworten von überrepräsentierten Gruppen (Anteil mit der entsprechenden Haltung unter den Befragten einer bestimmten Gruppe vs. Anteil mit dieser Haltung bei den übrigen Befragten); Schätzung der resultierenden Verzerrungen im Vergleich zu einer repräsentativen Stichprobe

Bezüglich der Haltungen in Sachen Data Governance sind kaum nennenswerte Unterschiede festzustellen. Der einzige Punkt, der ins Gewicht fallen dürfte, ist die Frage des Empowerments der Nutzer. Dieses wird von jenen Befragten, die beruflich mit Daten zu tun haben bzw. die in Betrieben mit Big Data arbeiten (beide überrepräsentiert), etwas weniger stark gewichtet als von jenen, bei denen dies nicht der Fall ist. Ebenso wird dieser Aspekt von den Beschäftigten der Privatwirtschaft (unterrepräsentiert) leicht höher gewichtet als von den Beschäftigten des öffentlichen Sektors. Die Diskrepanz in Bezug auf eine repräsentative Stichprobe dürfte daher bei etwas über 5 Prozentpunkten liegen, was den Wert noch näher an die 100%-Marke bringen würde. Ein minim geringerer Wert wäre dagegen bezüglich der Forderung zu erwarten, der Staat solle auf dem Datenmarkt regulierend eingreifen. Hier weisen Angestellte des öffentlichen Sektors und Mitarbeitende von Betrieben mit Big Data (beide überrepräsentiert) leicht höhere Werte auf als die übrigen Befragten.

Bezüglich der Einschätzung des kollektiven Handlungsbedarfs sind die grössten Abweichungen bei der Forderung nach einer Verschärfung der Datenschutzregeln und jener nach der Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) zu erwarten. In diesen Bereichen dürfte der Wert bei einer repräsentativen Umfrage 5 bzw. 10 Prozentpunkte höher liegen. Kaum ins Gewicht fallen dürften hingegen die Abweichungen hinsichtlich der Anzahl geforderter Massnahmen, da sich diese weitgehend neutralisieren, sowie die nur sehr geringe Abweichung hinsichtlich der Massnahmen zur Förderung der Sekundärnutzung von Daten.

Wir können demnach als Fazit festhalten, dass die Ergebnisse der vorliegenden Studie vermutlich nur in wenigen Punkten von den Ergebnissen einer hypothetischen Umfrage abweichen, die hinsichtlich der schweizerischen erwachsenen Gesamtbevölkerung repräsentativ ist. Konkret dürfte der Anteil an Befragten, welche die Chancen im Zusammenhang mit der Personalisierung und der Identifikation von „schwarzen Schafen“ positiv einschätzen, um rund 5 Prozentpunkte höher liegen. Bezüglich der Grundlagen der Data Governance fände das Prinzip des Empowerments der Nutzerinnen und Nutzer eine noch stärkere Unterstützung, während die Forderung nach einer staatlichen Intervention zur Regulierung des Datenmarkts etwas weniger stark unterstützt würde. Die Abweichungen dürften auch hier rund 5 Prozentpunkte betragen. Und schliesslich würden bei den Massnahmen die Forderung nach einer Verstärkung von Kontrollmechanismen und die Forderung nach einer Verschärfung der Datenschutzregeln höher gewichtet. Hier dürften sich die Abweichungen auf rund 10 bzw. auf rund 5 Prozentpunkte belaufen. Die Verzerrungen sind demnach übers Ganze gesehen gering und ändern nichts an der Tendenz der jeweiligen Ergebnisse, so dass die Repräsentativität der Studie in Bezug auf die schweizerische Gesamtbevölkerung weitgehend gegeben ist.

#### 7.10.5 Unterschiede hinsichtlich des politischen und zivilgesellschaftlichen Engagements

Abbildung 27 gibt einen Überblick über die Haltungen der Befragten bezüglich Big Data in Abhängigkeit von der thematischen Ausrichtung ihres zivilgesellschaftlichen Engagements. Aus der Abbildung ist ersichtlich, dass Big Data das grösste Potenzial von jenen Befragten zugeschrieben wird, welche angeben, dass sie sich im Rahmen ihres politischen oder zivilgesellschaftlichen Engagements mit Fragen der Weiterverwendung von personenbezogenen Daten oder mit Fragen des Konsumentenschutzes auseinandersetzen. Was die konkreten Auswirkungen von Big Data anbelangt, so bestehen unterschiedliche Einschätzungen bezüglich der Frage, ob Big Data die Gefahr von Manipulation erhöht. Entsprechende Befürchtungen hegen insbesondere jene Befragten, für die im Rahmen des politischen oder zivilgesellschaftlichen Engagements der Konsumentenschutz, die Förderung von Medien-, IT- und Datenkompetenz bzw. das Recht auf informationelle Selbstbestimmung eine wichtige Rolle spielen. Jene Befragten, die sich mit Fragen des Konsumentenschutzes und des Rechts auf informationelle Selbstbestimmung auseinandersetzen, sind auch am ehesten der Ansicht, dass Big Data die Privatsphäre bedroht und die Gefahr von Datendiebstahl, persönlicher Repression und Betrug erhöht. Eine besonders positive Sicht auf Big Data haben hingegen jene Befragten, welche sich mit Open Data, dem freien Zugang zu Wissen, der Innovationsförderung bzw. der Standortförderung auseinandersetzen.

Auswirkungen von Big Data	Datenschutz	Recht auf informationelle Selbstbestimmung	Freier Zugang zu Wissen	Open Data	Weiterverwendung von personenbezogenen Daten	Konsumerschutz	Förderung von Medien- / IT- / Datenkompetenz	Innovationsförderung	Standortförderung	Vertretung von Brancheninteressen
Big Data hat ein grosses Potenzial					41% vs 25%	43% vs 25%				
Big Data erhöht die Gefahr von Manipulation		71% vs 58%				79% vs 62%	77% vs 56%			
Big Data ermöglicht die Optimierung von Abläufen und erhöht die Agilität										
Big Data ermöglicht die Personalisierung und die Identifikation von 'schwarzen Schafen'										
Big Data bedroht die Privatsphäre und erhöht die Gefahr von Datendiebstahl, persönlicher Repression und Betrug		86% vs 75%				91% vs 79%				
Aus persönlicher Sicht überwiegen die Chancen von Big Data über die Risiken			56% vs 36%	59% vs 37%			62% vs 41%	62% vs 48%		
<b>Aspekte der Data-Governance</b>										
Der Staat muss intervenieren, weil der Datenmarkt nicht funktioniert.	84% vs 67%					88% vs 78%				
Der Datenschutz ist durch ein Empowerment der Nutzer sicherzustellen.										
Personendaten müssen geschützt werden; ihre Preisgabe kann problematisch sein.	89% vs 73%					95% vs 82%				
Die Leute erhalten für die Preisgabe ihrer Daten eine faire Gegenleistung.										
Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt.										
Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten ist nicht sinnvoll.							57% vs 39%		71% vs 42%	
<b>Kollektiver Handlungsbedarf</b>										
Anzahl geforderter Massnahmen (Massnahmen in über 15 Handlungsfeldern)	42% vs 26%		43% vs 24%			62% vs 28%	45% vs 33%			
Förderung der Sekundärnutzung von Daten			66% vs 50%	68% vs 49%			71% vs 53%		84% vs 61%	
Konsequente Umsetzung des Open-Data-Prinzips			80% vs 63%	84% vs 58%						
Verschärfung der Datenschutzregeln	55% vs 29%					65% vs 43%			41% vs 55%	
Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus)						82% vs 60%				
Datenschutzlabels, rechtliche Rahmenbedingungen für Datenzentren						85% vs 64%				
Standardisierung der technischen Schnittstellen										86% vs 64%
Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten	91% vs 78%		91% vs 80%	91% vs 83%	94% vs 85%	98% vs 84%				
<b>Verantwortung / Koordinationsebene</b>										
Der Staat muss handeln (Anteil, der bei über 50% der geforderten Massnahmen den Staat in der Pflicht sieht)			80% vs 91%							
Die Privatwirtschaft muss handeln (Anteil, der bei über 50% der Massnahmen die Privatwirtschaft in der Pflicht sieht)							43% vs 29%			
Die Zivilgesellschaft muss handeln (Anteil, der bei über 50% der Massnahmen die Zivilgesellschaft in der Pflicht sieht)					29% vs 18%					
Koordination auf regionaler / kant. Ebene (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf reg./kant. Ebene sieht)										
Koordination auf nationaler Ebene (Anteil der bei über 50% der Massnahmen einen Koordinationsbedarf auf nationaler Ebene sieht)										
Koordination auf europäischer Ebene (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf europäischer Ebene sieht)						41% vs 29%				
Koordination weltweit (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf europäischer Ebene sieht)	40% vs 19%	40% vs 25%					43% vs 28%			

Abbildung 27: Haltungen bezüglich Big Data in Abhängigkeit vom thematischen Fokus des politischen oder zivilgesellschaftlichen Engagements (Anteil mit der entsprechenden Haltung unter den Befragten mit einem bestimmten thematischen Fokus vs. Anteil mit dieser Haltung bei den Befragten ohne diesen thematischen Fokus)

Was die Ansichten hinsichtlich der Data Governance betrifft, so wird die Frage, ob der Staat intervenieren muss, weil der Datenmarkt nicht funktioniert, und die Frage, ob Personendaten unbedingt geschützt werden müssen, von Befragten, die sich mit Fragen des Konsumenten- und des Datenschutzes auseinandersetzen, eher bejaht, als von den übrigen. Demgegenüber halten vor allem Befragte, die sich der Vertretung von Brancheninteressen oder der Innovationsförderung widmen, eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten nicht für sinnvoll.

Den deutlich höchsten kollektiven Handlungsbedarf machen jene Befragten aus, die sich für den Konsumentenschutz einsetzen, gefolgt von jenen, die sich mit Fragen des Datenschutzes, des freien Zugangs zu Wissen und der Innovationsförderung auseinandersetzen. Dabei liegt die Förderung der Sekundärnutzung von Daten vor allem den Vertretern von Brancheninteressen am Herzen sowie den Befragten, die sich für die Innovationsförderung, Open Data oder den freien Zugang zu Wissen einsetzen. Eine konsequente Umsetzung des Open-Data-Prinzips wird insbesondere von den Befragten mit einem Bezug zu Open Data und dem freien Zugang zu Wissen gefordert. Demgegenüber stehen die Verfechter des Konsumentenschutzes an vorderster Stelle, wenn es darum geht, eine Verschärfung der Datenschutzregeln, eine Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) oder die Einführung von Datenschutzlabels zu fordern. Was die Verschärfung der Datenschutzregeln anbelangt, so sprechen sich ebenfalls die Verfechter von Datenschutzbelangen besonders prononciert dafür aus, während sich jene Befragten, die sich der Standortförderung widmen, eher dagegen aussprechen. Und schliesslich wird die Standardisierung von technischen Schnittstellen vor allem von den Vertretern von Branchen-Interessen gefordert, während sich bei der Forderung nach einem Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten eine Koalition zwischen Daten- und Konsumentenschützern sowie Verfechtern von Open Data (inklusive der freien Weiterverwendung von Personendaten) und des freien Zugangs zu Wissen abzeichnet.

Die Verantwortlichkeiten der verschiedenen Akteure werden von allen Gruppen sehr ähnlich eingeschätzt, wobei anzumerken ist, dass der Ruf nach staatlichem Handeln seitens jener Befragten am wenigsten oft ertönt, die sich für den freien Zugang zu Wissen einsetzen. Die Förderer von Medien-, IT- und Datenkompetenz sehen die Privatwirtschaft am stärksten in der Pflicht, und die Verfechter der Weiterverwendung von personenbezogenen Daten neigen am ehesten dazu, ein zivilgesellschaftliches Handeln zu fordern. Was die Koordinationsebene betrifft, so ist festzustellen, dass die Vertreter des Datenschutzes, des Konsumentenschutzes, die Verfechter des Rechts auf informationelle Selbstbestimmung sowie die Förderer von Medien-, IT- und Datenkompetenz am ehesten dazu neigen, bei der Umsetzung von Massnahmen eine Koordination auf internationaler Ebene zu fordern.

#### 7.10.6 Unterschiede hinsichtlich der Haltung bezüglich der Fragen der Data Governance

Wenn man einerseits die Befragten aufgrund ihrer Haltung in den Fragen der Data Governance gruppiert und sie mit den Bereichen in Beziehung setzt, in denen sie Handlungsbedarf verorten, lässt sich ein Bild davon zeichnen, welche Arten von Massnahmen mit welchen Haltungen bezüglich Data Governance korrelieren (siehe Abbildung 28). Hier zeigt sich, dass jene Befragten die meisten Massnahmen fordern, welche der Ansicht sind, dass der Staat intervenieren muss, weil der Datenmarkt nicht funktioniert, gefolgt von den Personen, die finden, dass Personendaten geschützt werden müssen, da ihre Preisgabe problematisch sein kann, dass der Datenschutz durch ein Empowerment der Nutzer sicherzustellen ist, bzw. dass die Einschätzung, welche Daten schützenswert sind, individuell variiert und auch kulturell geprägt ist. Bei den konkreten Massnahmen lassen sich zwei Cluster identifizieren: Eine Verschärfung der Datenschutzregeln, eine Verstärkung von Kontrollmechanismen, die Schaffung von Datenschutzlabels und ein Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten wird am stärksten von jenen Personen gefordert, die der Ansicht sind, dass der Staat intervenieren muss, weil der Datenmarkt nicht funktioniert, dass der Datenschutz durch ein Empowerment der Nutzer sicherzustellen ist und dass Personendaten geschützt werden müssen, da ihre Preisgabe problematisch sein kann. Das zweite Cluster betrifft die Forderung nach einer konsequenten Umsetzung des Open-Data-Prinzips und nach der Förderung der Sekundärnutzung von Daten. Diese Forderungen werden von jenen Befragten am stärksten unterstützt, die der Ansicht sind, dass die Leute für die Preisgabe ihrer Daten eine faire Gegenleistung erhalten, bzw. die in Sachen Datenschutz einen relativistischen Ansatz vertreten. Allerdings ist anzumerken, dass die Forderung nach einer konsequenten Umsetzung des Open-Data-Prinzips auch von jenen besonders

stark unterstützt wird, die den Datenschutz durch ein Empowerment der Nutzer sicherstellen wollen, oder die der Ansicht sind, dass der Staat intervenieren muss, weil der Datenmarkt nicht funktioniert.

	<i>Der Staat muss intervenieren, weil der Datenmarkt nicht funktioniert</i>	<i>Der Datenschutz ist durch ein Empowerment der Nutzer sicherzustellen</i>	<i>Personendaten müssen geschützt werden; ihre Preisgabe kann problematisch sein</i>	<i>Die Leute erhalten für die Preisgabe ihrer Daten eine faire Gegenleistung</i>	<i>Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt</i>	<i>Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten ist nicht sinnvoll</i>
<b>Kollektiver Handlungsbedarf</b>						
Anzahl geforderter Massnahmen (Masnahmen in über 15 Handlungsfeldern)	48% vs. 17%	42% vs. 21%	43% vs. 14%		43% vs. 33%	
Förderung der Sekundärnutzung von Daten				75% vs. 61%	66% vs. 56%	68% vs. 58%
Konsequente Umsetzung des Open-Data-Prinzips	73% vs. 61%	73% vs. 52%		84% vs. 69%	75% vs. 62%	
Verschärfung der Datenschutzregeln	60% vs. 25%	55% vs. 34%	58% vs. 21%			
Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus)	74% vs. 32%	69% vs. 37%	71% vs. 38%			
Datenschutzlabels, rechtliche Rahmenbedingungen für Datenzentren	79% vs. 52%	75% vs. 51%	76% vs. 53%			
Standardisierung der technischen Schnittstellen						
Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten	92% vs. 73%	91% vs. 61%	90% vs. 73%		92% vs. 82%	
<b>Verantwortung / Koordinationsebene</b>						
Der Staat muss handeln (Anteil, der bei über 50% der geforderten Massnahmen den Staat in der Pflicht sieht)	87% vs. 66%	84% vs. 67%	86% vs. 71%			
Die Privatwirtschaft muss handeln (Anteil, der bei über 50% der Massnahmen die Privatwirtschaft in der Pflicht sieht)	34% vs. 50%			52% vs. 35%	40% vs. 33%	
Die Zivilgesellschaft muss handeln (Anteil, der bei über 50% der Massnahmen die Zivilgesellschaft in der Pflicht sieht)						
Koordination auf regionaler / kant. Ebene (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf reg./kant. Ebene sieht)		10% vs. 20%				
Koordination auf nationaler Ebene (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf nationaler Ebene sieht)	80% vs. 69%					
Koordination auf europäischer Ebene (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf europäischer Ebene sieht)	33% vs. 21%					
Koordination weltweit (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf europäischer Ebene sieht)						

Abbildung 28: Kollektiver Handlungsbedarf, Verantwortung und Koordinationsebene in Abhängigkeit von den Haltungen hinsichtlich der Data Governance (Anteil mit der entsprechenden Haltung unter den Befragten mit einer bestimmten Einstellung bezüglich der Data Governance vs. Anteil mit dieser Haltung bei den Befragten, welche diese Einstellung bezüglich Data Governance nicht teilen)

Was die Verantwortlichkeiten anbelangt, so dürfte es nicht erstaunen, dass staatliches Handeln von jenen am stärksten gefordert wird, die der Ansicht sind, dass der Staat angesichts des Marktversagens auf dem Datenmarkt intervenieren muss. Diese Gruppe erwartet denn auch den geringsten Beitrag seitens der Privatwirtschaft. Staatliches Handeln wird aber auch von jenen verstärkt gefordert, die der Ansicht sind, dass der Datenschutz durch ein Empowerment der Nutzer sicherzustellen ist bzw. dass Personendaten geschützt werden müssen, da ihre Preisgabe problematisch sein kann. Im Gegensatz dazu sehen jene Befragten, welche der Ansicht sind, dass die Leute für die Preisgabe ihrer Daten eine faire Gegenleistung erhalten bzw. welche der Meinung sind, dass die Einschätzung, welche Daten schützenswert sind, individuell variiert und auch kulturell geprägt ist, die Privatwirtschaft am stärksten in der Pflicht.

### **7.11 Zusammenhang zwischen der Einschätzung der Auswirkung von Big Data und dem identifizierten Handlungsbedarf**

Abbildung 29 gibt einen Überblick über den Zusammenhang zwischen der Einschätzung der Befragten hinsichtlich der Auswirkungen von Big Data und dem identifizierten Handlungsbedarf. Wenig erstaunen dürfte, dass jene Befragten mehr Massnahmen fordern, welche Big Data ein grosses Potenzial (im Guten wie im Schlechten) zuschreiben. Dabei stehen die geforderten Massnahmen sowohl mit der Förderung der positiven Seiten von Big Data im Zusammenhang als auch mit der Verminderung der negativen Aspekte. Quasi ausschliesslich der Förderung der positiven Seiten von Big Data gilt die konsequente Umsetzung des Open-Data-Prinzips sowie die Förderung der Sekundärnutzung von Daten, während die Verschärfung der Datenschutzregeln und die Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus) in erster Linie mit der Abwendung von Risiken in Verbindung stehen. Interessanterweise werden die Schaffung von Datenschutzlabels und das Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten sowohl mit der Förderung der positiven Seiten als auch mit der Abwehr von Risiken in Verbindung gebracht. Jene Personen, die der Ansicht sind, dass die Chancen von Big Data aus persönlicher Sicht überwiegen, gehören zu den stärksten Verfechtern des Open-Data-Prinzips und der Förderung der Sekundärnutzung von Daten und fordern überdies häufiger als die übrigen eine Standardisierung der technischen Schnittstellen.

Was die Verantwortlichkeiten anbelangt, so steht der Ruf nach staatlichem Handeln in erster Linie in Beziehung mit der Abwehr von Risiken, während jene Befragten, aus deren persönlicher Sicht die Chancen von Big Data überwiegen, verstärkt die Privatwirtschaft in der Pflicht sehen. Bezüglich der bevorzugten Koordinationsebene lässt sich feststellen, dass die Gefahrenabwehr aus Sicht der Befragten neben der nationalen auch einer internationalen Koordination bedarf.

<b>Kollektiver Handlungsbedarf</b>	<i>Big Data hat ein grosses Potenzial</i>	<i>Big Data erhöht die Gefahr von Manipulation</i>	<i>Big Data ermöglicht die Optimierung von Abläufen und erhöht die Agilität</i>	<i>Big Data ermöglicht die Optimierung von "Schwarzen-Schafen"</i>	<i>Big Data bedroht die Privatsphäre und erhöht die Gefahr von Identifikation persönlicher Repräsentation und Betrug</i>	<i>Aus persönlicher Sicht überwiegen die Chancen von Big Data über die Risiken</i>
Anzahl geforderter Massnahmen (Massnahmen in über 15 Handlungsfeldern)	59% vs. 33%	45% vs. 30%	44% vs. 23%	47% vs. 30%	43% vs. 23%	
Förderung der Sekundämnutzung von Daten	68% vs. 60%		67% vs. 38%	67% vs. 55%	60% vs. 73%	74% vs. 51%
Konsequente Umsetzung des Open-Data-Prinzips	76% vs. 68%		74% vs. 56%	73% vs. 67%		77% vs. 63%
Verschärfung der Datenschutzregeln	69% vs. 47%	62% vs. 36%			58% vs. 30%	43% vs. 62%
Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus)	80% vs. 60%	76% vs. 48%			71% vs. 45%	59% vs. 74%
Datenschutzlabels, rechtliche Rahmenbedingungen für Datenzentren	83% vs. 68%	76% vs. 65%	75% vs. 62%	77% vs. 65%	76% vs. 57%	
Standardisierung der technischen Schnittstellen						74% vs. 64%
Empowerment der Nutzer mit Blick auf die Kontrolle von personenbezogenen Daten	95% vs. 85%	92% vs. 80%	90% vs. 81%	91% vs. 83%	90% vs. 75%	
<b>Verantwortung / Koordinationsebene</b>						
<b>Der Staat muss handeln</b> (Anteil, der bei über 50% der geforderten Massnahmen den Staat in der Pflicht sieht)	91% vs. 80%	86% vs. 76%			84% vs. 76%	79% vs. 87%
<b>Die Privatwirtschaft muss handeln</b> (Anteil, der bei über 50% der Massnahmen die Privatwirtschaft in der Pflicht sieht)						43% vs. 32%
<b>Die Zivilgesellschaft muss handeln</b> (Anteil, der bei über 50% der Massnahmen die Zivilgesellschaft in der Pflicht sieht)						
<b>Koordination auf regionaler / kant. Ebene</b> (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf reg./kant. Ebene sieht)		9% vs. 14%			10% vs. 16%	
<b>Koordination auf nationaler Ebene</b> (Anteil der bei über 50% der Massnahmen einen Koordinationsbedarf auf nationaler Ebene sieht)						
<b>Koordination auf europäischer Ebene</b> (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf europäischer Ebene sieht)	39% vs. 28%	33% vs. 25%		34% vs. 27%	32% vs. 24%	
<b>Koordination weltweit</b> (Anteil, der bei über 50% der Massnahmen einen Koordinationsbedarf auf europäischer Ebene sieht)	51% vs. 35%	44% vs. 30%			41% vs. 31%	36% vs. 43%

Abbildung 29: Kollektiver Handlungsbedarf, Verantwortung und Koordinationsebene in Abhängigkeit von den Einschätzungen der Auswirkungen von Big Data (Anteil mit der entsprechenden Haltung unter den Befragten mit einer bestimmten Ansicht bezüglich den Auswirkungen von Big Data vs. Anteil mit dieser Haltung bei den Befragten, welche diese Ansicht bezüglich den Auswirkungen von Big Data nicht teilen)

## 8 Implikationen für eine „Good Data Governance“

Ausgehend von den Ergebnissen der Experten-Interviews haben wir im Hinblick auf eine „Good Data Governance“ sieben Thesen formuliert (siehe Kapitel 6), die wir nun im Lichte der Ergebnisse der Online-Befragung diskutieren möchten.

### 8.1 Der Datenschutz im Umbruch

#### These 1

#### Beim Datenschutz braucht es einen Paradigmenwechsel.

Dass es einen Paradigmenwechsel braucht, ist weitgehend unbestritten. Wie dieser aus-  
schauen soll ist noch unklar. Aufgrund der geführten Gespräche lassen sich folgende  
Tendenzen ausmachen:

**Empowerment der Nutzer:** Die Preisgabe und Nutzung von personenbezogenen Daten  
muss durch die betroffenen Personen effektiv kontrolliert werden können.

**Recht auf Anonymität:** Elementare Transaktionen des Lebens müssen auch anonym  
abgewickelt werden können.

**Technische Massnahmen:** Der Datenschutz ist insbesondere auch durch technische  
Massnahmen sicherzustellen.

**Wettbewerbsrechtlicher Ansatz:** Wenn wir einen besseren Schutz der Privatsphäre  
erreichen wollen, reicht es nicht, beim Datenschutz anzusetzen, sondern es braucht  
auch Massnahmen im Bereich der Wettbewerbsaufsicht.

Des Weiteren ist angesichts der Entwicklungen im Big-Data-Bereich die Frage des  
Datenschutzes insbesondere auch mit Blick auf die vermehrte Zusammenführung von  
Daten aus ganz unterschiedlichen Quellen und die damit verbundene Möglichkeit der  
De-Anonymisierung von Personendaten neu zu beurteilen.

Tabelle 10: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 1

Wie die Umfrageergebnisse zeigen, ist ein effektiver Schutz der Personendaten das A und O für einen  
Umgang mit Big Data, der am Ende der Gesellschaft einen Nutzen bringt, denn mit dem positiven Po-  
tential von Big Data sind auch erhöhte Risiken hinsichtlich der missbräuchlichen Verwendung von Da-  
ten verbunden. Big Data wird daher von einer grossen Mehrheit der Befragten mit einer grund-  
sätzlichen Bedrohung der Privatsphäre in Verbindung gebracht. Wie im Rahmen der qualitativen  
Befragungen angemerkt wurde, nimmt durch Big Data nicht nur die Gefahr von Missbräuchen zu,  
sondern es steigt auch das potentielle Schadensausmass. Aufgrund der Ergebnisse der qualitativen  
Befragung haben wir die These formuliert, dass es angesichts der Entwicklungen im Zusammenhang  
mit Big Data beim Datenschutz einen Paradigmenwechsel braucht. Anhand der Umfrageergebnisse  
können wir nun genauer präzisieren, wie dieser Paradigmenwechsel aussehen könnte:

Zunächst ist einmal festzuhalten, dass eine grosse Mehrheit der Befragten den Schutz von Personen-  
daten als sehr wichtig erachtet. Zudem wird auch dem Aspekt der Richtigkeit der personenbezogenen  
Daten eine sehr hohe Bedeutung beigemessen. Als nicht mehr zeitgemäss erscheint die traditionelle  
Unterscheidung zwischen besonders schützenswerten Daten und weniger schützenswerten Personen-  
daten. Dafür dürften zwei Gründe verantwortlich sein: Erstens hat aufgrund der vermehrten Zusam-  
menführung von Daten aus ganz unterschiedlichen Quellen die Gefahr der De-Anonymisierung von  
vordergründig anonymisierten Daten eine ganz neue Dimension erhalten. So gilt es aus Sicht von drei  
Vierteln aller Befragten, jene Daten besonders zu schützen, welche es erlauben, jemanden zu identi-  
fizieren, wobei das Verbinden von Personendaten aus unterschiedlichen Quellen in einem Personen-  
profil als besonders problematisch erachtet wird. Zweitens hat sich bei einer Mehrheit der Befragten  
die Überzeugung durchgesetzt, dass die Einschätzung, welche Daten schützenswert sind, individuell  
variiert und auch kulturell geprägt ist. D.h. es wäre durchaus denkbar, dass a priori sensible Daten

(wie z.B. Gesundheitsdaten) von den Betroffenen mehr oder weniger anonymisiert weitergegeben und zur Weiterverwendung freigegeben werden. Dabei müsste aber jeder Einzelne die Kontrolle darüber behalten, wer welche Daten zu welchem Zweck erheben, beziehen und zusammenführen darf, womit wir beim Ansatz der persönlichen Datenhoheit wären. Ein entsprechendes Empowerment der Nutzerinnen und Nutzer wird von den Umfrageteilnehmenden grossmehrheitlich unterstützt. Zudem dürfte es auch bei der Wirtschaft auf Zustimmung stossen. Zur Umsetzung des Prinzips der persönlichen Datenhoheit sollen im Bereich der personenbezogenen Daten neue Eigentums- und Nutzungsrechte definiert werden. Zudem sollen Mechanismen geschaffen und Dienste bereitgestellt werden, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben.

Was die Sicherstellung des Schutzes der Personendaten betrifft, herrscht Einigkeit darüber, dass technische Massnahmen für den Datenschutz eine wichtige Rolle spielen. Dieser Punkt dürfte auch bei der Wirtschaft auf Unterstützung stossen. Aus Sicht der Bürgerinnen und Nutzerinnen erscheint es zudem als wünschenswert, den Datenschutz auch mittels juristischer und ökonomischer Massnahmen, wie Auflagen, Inspektionen und Bussen sicherzustellen. Die Umfrageergebnisse lassen vermuten, dass diese Sicht auch von der Wirtschaft mehrheitlich geteilt wird, wenn ihr auch die Grossfirmen kritisch gegenüberstehen dürften. Dasselbe gilt für die Forderung, dass die Geschäftspraktiken der Internet-Riesen stärker reguliert und kontrolliert werden sollen. Eine Mehrheit der Befragten fordert eine Verschärfung der Datenschutzregeln für die Privatwirtschaft und eine verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich. Während eine Verschärfung der Datenschutzregeln auf nationaler Ebene wohl umsetzbar wäre, ist eine Koordination auf internationaler Ebene angezeigt, um Marktverzerrungen vorzubeugen. Bei der wettbewerbsrechtlichen Kontrolle von (Quasi-)Monopolisten im Internet-Bereich scheint ein koordiniertes Vorgehen auf internationaler Ebene geradezu unerlässlich. Ob sich diese Verschärfung der Datenschutzregeln und der wettbewerbsrechtlichen Kontrollen realisieren lässt, dürfte daher primär davon abhängen, ob es gelingt, auf dem internationalen Parkett den Interessen der Menschen trotz gegenläufiger Interessen von internationalen Grossfirmen Gehör zu verschaffen.

Als Fazit kann festgehalten werden, dass die These der Notwendigkeit eines Paradigmenwechsels beim Datenschutz von den Umfrageergebnissen gestützt wird. Dabei scheinen sich alle vier im Rahmen der qualitativen Befragungen identifizierten Tendenzen zu bestätigen (siehe Tabelle 10: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 1). Überdies geht aus der Umfrage ganz klar hervor, dass der Datenschutz angesichts der Entwicklungen im Bereich von Big Data insbesondere mit Blick auf die privatwirtschaftlichen Akteure gestärkt werden muss.

## 8.2 Aufbau und Pflege einer gemeinsamen Daten-Infrastruktur

### These 2 **Der gesellschaftliche Nutzen von Daten erhöht sich, wenn sie als freie Infrastruktur-Ressourcen verfügbar sind.**

Dies gilt sowohl für nicht-personenbezogene Daten als auch für personenbezogene Daten.

**Open-Data-Prinzip:** Bei den nicht-personenbezogenen Daten führt die konsequente Anwendung des Open-Data-Prinzips zum grössten gesellschaftlichen Nutzen. Nicht-personenbezogene Daten sollen grundsätzlich zur freien Weiterverwendung zur Verfügung stehen. Ausnahmen sind Geschäftsgeheimnisse, sicherheitsrelevante Daten und urheberrechtlich geschützte Daten.

**Offene Personendaten:** Personenbezogene Daten sollen von den Betroffenen – je nach persönlichem Gutdünken – zur Weiterverwendung durch Dritte freigegeben werden. Hier ist ein Empowerment der Nutzerinnen und Nutzer vonnöten, so dass diese über ihre Personendaten verfügen und sie in Kenntnis des Verwendungszwecks gezielt für die Weiterverwendung freigeben können. Entsprechende Plattformen, welche die Freigabe und das Pooling von personenbezogenen Daten erleichtern, sind aus den USA und Grossbritannien bereits bekannt. Hier ist es wichtig, dass beispielsweise Bankdaten oder Gesundheitsdaten von den jeweiligen Dienstleistern in einem standardisierten Datenbezugsformat bereitgestellt werden, so dass sie von den Daten-Eignern (d.h. den Nutzerinnen und Nutzern) einfach gepoolt werden können, damit darauf aufbauend neuartige Dienstleistungen erbracht werden können. Denkbar sind beispielsweise Vergleichsdienste, Dienste zur Verhaltensbeeinflussung (z.B. Energieverbrauch, Bewegung, usw.) sowie personalisierte Angebote jeglicher Art. Darüber hinaus können die personenbezogenen Daten für Forschungszwecke freigegeben werden (z.B. für die medizinische Forschung).

Tabelle 11: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 2

Das Open-Data-Prinzip stösst bei den Umfrageteilnehmenden auf breite Unterstützung. Zur freien Weiterverwendung bereitgestellt werden sollen insbesondere Forschungsdaten. Dabei sehen die Befragten nicht nur den Staat, sondern auch die Privatwirtschaft in der Pflicht. Des Weiteren wird von knapp zwei Dritteln der Befragten Wert darauf gelegt, dass das Open-Data-Prinzip in der öffentlichen Verwaltung konsequent umgesetzt wird, während gut die Hälfte wünscht, dass dies mit Blick auf sämtliche Daten geschieht, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor). Bei den nicht-personenbezogenen Daten wird demnach eine möglichst breite Umsetzung des „Open Government Data“- und des „Open Research Data“-Prinzips gefordert, welche teilweise auch den privaten Sektor mit einbezieht.

Eine Generalisierung des Open-Data-Prinzips – im Sinne, dass ein Maximum an Daten im Internet zur allgemeinen Weiterverwendung bereitgestellt werden soll – ist jedoch umstritten. Vorbehalte bestehen insbesondere mit Blick auf das Verfügbarmachen von Personendaten: Gut die Hälfte der Befragten findet es problematisch, wenn zu viele Menschen ihre persönlichen Daten aus individuellen Nutzenüberlegungen heraus preisgeben. Zudem fehlen heute die Voraussetzungen, die es dem Einzelnen erlauben würden, seine persönliche Datenhoheit auch effektiv auszuüben. Bevor daran gedacht werden kann, „offene“ Personendaten breitflächig zu propagieren, müssen daher eine Reihe von Hürden überwunden werden: Das im vorigen Abschnitt beschriebene Empowerment der Bürgerinnen, Kundinnen und Nutzerinnen muss erst einmal erreicht werden. Dazu bedarf es nicht nur einer Verstärkung des Datenschutzes, sondern es gilt auch Marktungleichgewichte infolge von Informations-Asymmetrien und natürlichen Monopolen zu beseitigen und die Betroffenen mittels Aufklärungs- und Sensibilisierungsmassnahmen dafür zu gewinnen, innerhalb der Datenwelt eine aktivere Rolle zu spielen.

### 8.3 Risiken von Big Data

#### These 3

#### **Big Data verschärft eine Reihe von Gefahren, die abgewehrt werden müssen.**

Durch Big Data erhöht sich nicht nur die Wahrscheinlichkeit einer missbräuchlichen oder unerwünschten Nutzung oder Verknüpfung von Daten, sondern auch das damit verbundene Schadenspotential. Grundsätzlich lassen sich vier Arten von Gefahren unterscheiden: **staatliche Repression, ökonomische Diskriminierung, persönliche Repression** (diese lässt sich unter Umständen durch staatliche Repression oder ökonomische Diskriminierung institutionalisieren) sowie die **unkontrollierte Eigendynamik der Systeme** (Gefahr von Algorithmen, die man nicht mehr richtig versteht und beherrscht).

Tabelle 12: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 3

Dass Big Data eine Reihe von beträchtlichen Risiken mit sich bringt, ist unter den Befragten weitestgehend unbestritten. Bezeichnend ist auch, dass insbesondere jene Personen, welche Big Data ein grosses Nutzenpotential zuschreiben, damit auch grosse Risiken in Verbindung bringen. Im Vordergrund stehen die grundsätzliche Bedrohung der Privatsphäre und die missbräuchliche Verwendung von Daten, inklusive Datendiebstahl. Rund 60% der Befragten sind zudem der Ansicht, dass Big Data eine erhöhte Gefahr von ökonomischer Diskriminierung mit sich bringt. Ebenso viele befürchten, dass Big Data dazu führt, dass es beim Fällen von Entscheiden, zu einer übertriebenen Fokussierung auf Daten kommt. Etwas weniger ausgeprägt, aber dennoch nicht zu vernachlässigen sind die Bedenken der Befragten hinsichtlich der unkontrollierten Eigendynamik der Systeme, der erhöhten Gefahr von persönlicher Repression und von Täuschungsdelikten, der Verschärfung von politischen und ökonomischen Machtgefällen sowie hinsichtlich der erhöhten Gefahr von politischer Manipulation und von staatlicher Repression.

Aus Sicht der Befragten sollten die Gefahren von Big Data dadurch vermindert werden, dass im Bereich der personenbezogenen Daten neue Eigentums- oder Nutzungsrechte definiert werden und zur Sicherstellung des Datenschutzes technische Lösungen zur Anwendung kommen. Im Rahmen der qualitativen Befragung wurde in diesem Zusammenhang von gewissen Experten die Vorstellung geäußert, dass die Menschen die Herrschaft über die eigenen personenbezogenen Daten behalten und diese in einem Daten-Tresor bei einer Daten-„Bank“ hinterlegen sollten. Dort wären die Daten durch technische Vorkehrungen gesichert, so dass es beispielsweise nachvollziehbar wäre, wer wann darauf zugegriffen hat. Im Vergleich zur Funktionsweise heutiger Datenmonopoldienste, wie Amazon, Facebook, Apple oder Google, würde die Datenbesitzlage umgekehrt, ohne dass die Funktionalität dadurch reduziert würde. Dank virtueller Agenten und intelligenter Schnittstellen würden nämlich personalisierte Angebote weiterhin ermöglicht, ohne dass aber alle Profildaten durch einen Akteur zentral kontrolliert würden. Quasi ergänzend zu diesen rechtlichen und technischen Massnahmen fordern die Befragten Aufklärungs- und Sensibilisierungsmassnahmen, eine verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich sowie eine Verschärfung der Datenschutzregeln für die Privatwirtschaft im Allgemeinen.

Wie im Rahmen der qualitativen Befragung vereinzelt zum Ausdruck gebracht wurde, kann das steigende Gefahrenbewusstsein im Zusammenhang mit Big Data auch als Anlass genommen werden, für Schweizer Unternehmen und/oder Genossenschaften neue wirtschaftliche Tätigkeitsfelder zu eröffnen, indem sichere Datenzentren angeboten werden. Entsprechend wünschen sich zwei Drittel der Befragten eine Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren.

## 8.4 Big Data und gesellschaftliche Ungleichgewichte

### These 4

**Machtgefälle aufgrund von einseitiger Datenkontrolle gilt es zu vermeiden.**

Mittel zur Reduktion von Machtgefällen sind die Umsetzung des **Transparenz-Prinzips** (alle Daten von politischer Relevanz müssen offen zugänglich sein), die **Kontrolle bzw. die Zerschlagung von Monopolen/Oligopolen** sowie der **Schutz vor staatlichem Missbrauch von Personendaten**. Hinsichtlich des letzten Punktes ist es wichtig, dass der Kampf gegen den Terrorismus oder andere Missstände nicht als Vorwand dienen, um die Schutzmechanismen gegen staatlichen Missbrauch von Personendaten abzubauen.

Tabelle 13: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 4

Das bestehende Machtgefälle ist aus Sicht der Befragten insbesondere auf dem sogenannten „Daten-Markt“ problematisch, wo es dazu führt, dass die Kunden/Nutzer nicht in der Lage sind, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen. Damit verbunden ist auch eine erhöhte Gefahr der ökonomischen Diskriminierung. In der Konsequenz wird gegenüber den (Quasi-) Monopolisten im Internet-Bereich ein härteres Durchgreifen seitens der Wettbewerbsaufsicht gefordert. Im Rahmen der qualitativen Befragung wurde in diesem Zusammenhang auch mehrfach darauf hingewiesen, dass die Nutzerinnen und Nutzer von den Anbietern von Online-Diensten oftmals vor die Alternative gestellt werden, die geltenden Nutzungsbedingungen nolens volens zu akzeptieren oder auf die Nutzung des Dienstes gänzlich zu verzichten. Dies steht in eklatantem Widerspruch zur persönlichen Datenhoheit, wie sie von den Befragten grossmehrheitlich gefordert wird.

Das Schutzbedürfnis gegenüber Machtexzessen seitens des Staates scheint unter den Befragten etwas weniger ausgeprägt zu sein als gegenüber jenen der Privatwirtschaft, wobei sich hier die Beschäftigten der Privatwirtschaft kritischer zeigen als die im öffentlichen Sektor tätigen Umfrageteilnehmer: 61% sprechen sich für mehr Transparenz im öffentlichen Sektor aus, indem das Open-Data-Prinzip auf sämtliche Informationen angewendet wird, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive der Daten der Privatwirtschaft). Und 45% befürchten, dass die Gefahr von staatlicher Repression infolge von Big Data zunehmen wird; das sind ebenso viele, wie mit einer erhöhten Gefahr von persönlicher Repression rechnen.

## 8.5 Marktprinzip und Empowerment der Nutzer

### These 5

#### Es sollte ein liberaler Ansatz verfolgt werden.

Dieser kennzeichnet sich durch die konsequente Anwendung des **Markt-Prinzips** und eine **Befähigung der Nutzer**. Ein liberaler Ansatz basiert auf den Prämissen, dass sich Datenschutz und Data-Sharing über Marktmechanismen regulieren lassen und dass Nutzerinnen und Nutzer mittels geeigneter Software-Lösungen, Transparenz-Auflagen für Unternehmen sowie Aufklärungs- und Bildungsmaßnahmen dazu gebracht werden können, einen bewussten und informierten Umgang mit ihren Daten zu pflegen.

Tabelle 14: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 5

80% der Befragten sind davon überzeugt, dass Kunden/Nutzer heute nicht in der Lage sind, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen. Das Markt-Prinzip mag in gewissen Teilsektoren funktionieren, in denen mehrere Anbieter leicht substituierbare Güter anbieten und der Wettbewerb derart spielt, dass sich keiner der Anbieter eine Verletzung seiner Datenschutzpflichten erlauben kann, ohne gleich Marktanteile an die Konkurrenz zu verlieren. Dabei müsste der Wettbewerb auch hinsichtlich der Gegenleistungen spielen, die man im Gegenzug für die Preisgabe seiner Daten erhält. Allerdings scheint dieses Modell heute eher Utopie als Realität zu sein, denn Informations-Asymmetrien und natürliche Monopole, die infolge von Netzwerkeffekten entstehen, führen aus Sicht einer klaren Mehrheit der Umfrageteilnehmer dazu, dass der Datenmarkt in etlichen Bereichen versagt.

In der allgemeinen Tendenz deuten die Befragungsergebnisse jedoch darauf hin, dass die Befragten sich mehrheitlich ein System wünschen, bei dem der Markt dank eines Empowerment der Nutzerinnen und Nutzer und einer stärkeren Regulierung und Kontrolle der privatwirtschaftlichen Akteure durch den Staat besser funktioniert als heute. Damit steht als Ziellösung ganz klar ein liberaler Ansatz im Vordergrund. Einer weitergehenden, direkten Einmischung des Staates auf dem Datenmarkt wird eher mit Skepsis begegnet.

## 8.6 Staatliche Intervention

### These 6

#### **Staatliche Intervention ist nötig.**

Die Notwendigkeit von staatlichen Interventionen ergibt sich aus dem **Marktversagen** und der **Überforderung der Nutzer**. In etlichen Bereichen ist zu beobachten, dass der Daten-Markt aufgrund von natürlichen Monopolen, Informations-Asymmetrien und negativen Externalitäten versagt. Zudem sind Kunden bzw. Nutzer nicht in der Lage, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen.

Tabelle 15: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 6

Die Umfrageergebnisse deuten darauf hin, dass ohne ein starkes Engagement des Staates die Entwicklung im Zusammenhang mit Big Data aus dem Ruder laufen wird. Bezeichnenderweise sehen dies die im privaten Sektor tätigen Personen genauso wie die Angestellten des öffentlichen Sektors. Die Befragten lassen keinen Zweifel daran, dass der heutige Datenmarkt aus ihrer Sicht versagt. Gründe dafür sind Informations-Asymmetrien und natürliche Monopole sowie – in einem etwas geringeren Masse – negative Externalitäten im Zusammenhang mit der Preisgabe von persönlichen Daten.

Zunächst wird vom Staat erwartet, dass er regulierend tätig wird. Gefordert werden insbesondere:

- die Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten;
- eine Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren;
- eine verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich; sowie
- eine Verschärfung der Datenschutzregeln für die Privatwirtschaft.

Des Weiteren soll er die Nutzerinnen und Nutzer über die Chancen und Gefahren im Zusammenhang mit Big Data aufklären und durch Sensibilisierungsmassnahmen zum Empowerment der Nutzer beitragen. Und schliesslich soll er das Angebot von Daten fördern, indem er das Open-Data-Prinzip in der öffentlichen Verwaltung konsequent umsetzt und auf sämtliche Daten anwendet, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor).

Daneben wird vom Staat erwartet, dass er sich Seite an Seite mit der Privatwirtschaft dafür einsetzt, dass:

- Mechanismen geschaffen werden, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben;
- Dienste bereitgestellt werden, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen;
- das Open-Data-Prinzip im Bereich der Forschung konsequent umgesetzt wird;
- die Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes gefördert wird;
- die Standardisierung von technischen Schnittstellen vorangetrieben wird; und
- die Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.) gefördert wird.

## 8.7 Die internationale Dimension

### These 7

#### **Data Governance muss im internationalen Kontext angegangen werden.**

Die Hauptgefahr in Sachen Datenschutz geht von **multinationalen Grossfirmen** aus, gegen die einzelne Staaten nicht viel ausrichten können. Zudem führen einzelstaatliche Lösungen auf internationalen Märkten zu **Wettbewerbsverzerrungen** und im Endeffekt zu einer Verwässerung der Standards. Die Situation verschärft sich dadurch, dass digitalen Daten heute kein geographischer Ort mehr zukommt, da sie weltweit verteilt sind.

Tabelle 16: Sieben Thesen hinsichtlich einer „Good“ Data Governance: These 7

Aus der Sicht der Mehrheit der Befragten muss das Vorgehen gegenüber den multinationalen Grossunternehmen in der Tat primär auf internationaler Ebene koordiniert werden. Bei den meisten übrigen Massnahmen wird jedoch der Koordination auf Bundesebene ein grösseres Gewicht beigemessen als der Koordination auf internationaler Ebene, auch wenn letztere mit Blick auf die meisten der geforderten Massnahmen aus Sicht der Befragten ebenfalls eine wichtige Rolle spielt. – Eine Ausnahme bildet die konsequente Umsetzung des Open-Data-Prinzips in der öffentlichen Verwaltung; diese kann aus Sicht der Umfrageteilnehmer ohne grosse Koordination mit dem Ausland erfolgen.

## 9 Fazit und Ausblick

Beim Phänomen „Big Data“ handelt es sich um eine allmähliche Entwicklung infolge grösserer Analyse- und Speicherkapazitäten, die sich dadurch manifestiert, dass immer grössere Mengen von teils heterogenen Daten verarbeitet und miteinander verknüpft werden. Damit handelt es sich bei Big Data um eine Entwicklung, die nach und nach immer weitere Bereiche der Wirtschaft und Gesellschaft erreicht.

Big Data bringt bedeutende Chancen und Vorteile mit sich, wie zum Beispiel das Gewinnen neuer Erkenntnisse und Entdecken neuer Zusammenhänge, die Personalisierung von Angeboten und Informationen, verbesserte Prognosen in ganz unterschiedlichen Bereichen, eine erhöhte Agilität von Unternehmen und Organisationen, die Optimierung von Abläufen sowie die Möglichkeit, Entscheide vermehrt faktenbasiert zu fällen.

Allerdings setzt die erfolgreiche Anwendung von Big Data in Unternehmen organisatorische Anpassungen und einen kulturellen Wandel voraus. Die Experten-Interviews haben gezeigt, dass sich einige Unternehmen und Organisationen bereits an die neuen Gegebenheiten angepasst haben, während sich andere erst anschicken, auf den Big-Data-Zug aufzuspringen.

Die Studie hat aber auch gezeigt, dass die gesellschaftlichen Implikationen von Big Data stärker in den Fokus genommen werden sollten. Die drängendsten Fragen stellen sich im Bereich des Schutzes von Personendaten bzw. bei der Prävention von Daten-Missbrauch. Einzelne Stimmen warnen zudem vor der unkontrollierten Eigendynamik der Systeme, wenn immer mehr Entscheide auf Algorithmen basieren, die niemand mehr richtig versteht und beherrscht. Ein weiterer Problembereich, für den Big Data nicht ursächlich ist, auf den sich Big Data aber verschärfend auswirken dürfte, ist die ungleiche Verteilung von Ressourcen und Macht, welche die Gefahr von gesellschaftlichen Verwerfungen birgt, falls nicht rechtzeitig Gegensteuer gegeben wird.

Neben der Abwehr von Gefahren sollte auch die Förderung des Potentials von Big Data nicht zu kurz kommen. Hier herrscht weitgehend Einigkeit darüber, dass der gesellschaftliche Nutzen von Daten sich erhöht, wenn sie als freie Infrastruktur-Ressourcen verfügbar sind und von den verschiedenen Akteuren möglichst unkompliziert weiterverwendet werden können. Dies gilt in erster Linie für nicht-personenbezogene Daten; bei den personenbezogenen Daten ist die Situation komplizierter, da es zunächst neuer Mechanismen bedarf, die es den Einzelnen erlauben, die Kontrolle über ihre Daten effektiv wahrzunehmen und die Daten gezielt – und nicht völlig unkontrolliert, wie dies heute oftmals geschieht – für bestimmte Zwecke zur Weiterverwendung zur Verfügung zu stellen.

Wie aus den Umfrageergebnissen hervorgeht, stellt sich die grundsätzliche Herausforderung, die Entwicklungen im Bereich Big Data so zu kanalisieren, dass sie zum Nutzen der Menschen reichen. Heute scheinen vor allem grössere Unternehmen von Big Data zu profitieren, während die Befragten die Situation aus ihrer persönlichen Sicht eher kritisch beurteilen und ein starkes Engagement des Bundes fordern, um die Situation nicht aus dem Ruder laufen zu lassen. Dabei erscheint eine Dreipunkte-Strategie angezeigt:

- 1) **Aufbau und Pflege einer nationalen Dateninfrastruktur:** Die positive Wirkung von Big Data kann durch die Bereitstellung von Daten als Infrastrukturrressource zur freien Weiterverwendung verstärkt werden. Es gilt daher, dem im Rahmen der bundesrätlichen Open-Government-Data-Strategie etablierten Open-Data-Prinzip über die gesamte Verwaltung hinweg, in der Forschung und teilweise auch in der Privatwirtschaft zum Durchbruch zu verhelfen und es konsequent umzusetzen. Zudem sollte in enger Zusammenarbeit mit der Privatwirtschaft die Standardisierung von technischen Schnittstellen vorangetrieben und die Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists u.ä.) gefördert werden. Ziel sollte es sein, eine national koordinierte und international vernetzte Dateninfrastruktur zu schaffen.

- 2) **Massnahmen zum Schutz vor Missbräuchen:** Um Missbräuchen und Ungleichgewichten entgegenzuwirken, sollten die Datenschutzregeln für die Privatwirtschaft verschärft, die wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internetbereich verstärkt und Aufklärungs- und Sensibilisierungsmassnahmen durchgeführt werden. Zudem müssen die rechtlichen Rahmenbedingungen für sichere Datenzentren verbessert werden. In enger Kooperation mit der Privatwirtschaft sollten zudem vermehrt technische Lösungen entwickelt werden, um den Datenschutz sicherzustellen. Viele dieser Massnahmen weisen allerdings die Schwierigkeit auf, dass sie international koordiniert werden müssen, um wirksam zu sein.
- 3) **Umsetzung des Prinzips der persönlichen Datenhoheit:** Als langfristige Lösung sollte die Vision der „My Data“-Initiative verfolgt und beim Datenschutz ein Paradigmenwechsel eingeleitet werden, indem die Menschen befähigt werden, die Kontrolle über ihre Daten besser auszuüben. Zur Umsetzung des Prinzips der persönlichen Datenhoheit müssen im Bereich der personenbezogenen Daten neue Eigentums- und Nutzungsrechte definiert werden. Zudem gilt es, in enger Kooperation mit der Privatwirtschaft Mechanismen zu schaffen und Dienste bereitzustellen, welche es den Einzelnen erlauben, ihre personenbezogenen Daten – unter grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben. Auch hier ist eine internationale Koordination der Anstrengungen unerlässlich. Während die Realisierung dieses liberalen Ansatzes zur Behebung der Ungleichgewichte auf dem Datenmarkt heute noch in weiter Ferne liegen mag, geniesst er als Zielvorgabe bei allen Anspruchsgruppen breite Unterstützung.

Während die Massnahmen in Punkt 1) die Förderung der positiven Aspekte von Big Data bezwecken und die Massnahmen in Punkt 2) die negativen Auswirkungen von Big Data einzudämmen suchen, setzen die Massnahmen in Punkt 3) wichtige Eckpfeiler der künftigen Data-Governance. Dabei spielt das Prinzip der persönlichen Datenhoheit eine doppelte Rolle: Einerseits dient es als Leitvision bei der Ausgestaltung der Massnahmen zur Gefahren-Abwehr, und andererseits ist es der Schlüssel für die künftige Einbindung von personenbezogenen Daten in die gemeinsame Daten-Infrastruktur. Aus den Umfrageergebnissen geht unmissverständlich hervor, dass die Forderung nach staatlicher Intervention nicht dem Wunsch nach einer Bevormundung der Bürger oder einer Gängelung der Privatwirtschaft entspringt. Im Gegenteil: Ziel ist es, durch ein System von Schutz- und Kontrollmechanismen ein Empowerment der Bürger und ein besseres Funktionieren der Märkte zu ermöglichen. Dabei sollte auch der Schutz vor staatlichem Missbrauch nicht zu kurz kommen.

Wie ein Umfrageteilnehmer in seinem Kommentar bemerkte, wurden mit der vorliegenden Studie hinsichtlich des Umgangs mit Big Data das „Was?“ geklärt und die Prioritäten gesetzt; nun gilt es, das „Wie?“ zu klären und dem identifizierten Handlungsbedarf mit konkreten Massnahmen zu begegnen. Angesichts der Tatsache, dass im Hinblick auf die Umsetzung etlicher Massnahmen eine internationale Koordination angezeigt ist, liegt es nahe, sich von Lösungsansätzen, welche in anderen Ländern verfolgt werden, inspirieren zu lassen. Der unlängst erschienene Bericht der OECD zu „Data Driven Innovation“ kann hierzu einen ersten Überblick bieten (OECD 2015).

## 10 Literaturverzeichnis

- Berinato, S. (2014). With Big Data Comes Big Responsibility. *Harvard Business Review*, 92(11), 100–104. Online: <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=98971602&site=ehost-live>
- Bryant, R., Katz, R., & Lazowska, E. (2008). Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society. *Computing Research Association*, 1–15. Online: <http://www.just.edu.jo/~amerb/teaching/2-12-13/cs728/20123173012.pdf>
- Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS QUARTERLY*, 36(4), 1165–1188.
- Cox, M., & Ellsworth, D. (1997). Application-controlled demand paging for out-of-core visualization. *Proceedings. Visualization '97 (Cat. No. 97CB36155)*. doi:10.1109/VISUAL.1997.663888
- Davenport, T. H., & Patil, D. J. (2012). Data scientist: the sexiest job of the 21st century. *Harvard Business Review*, 90(10).
- Eisenstein, E. L. (1993). *The Printing Revolution in Early Modern Europe*. Cambridge University Press.
- El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A Systematic Review of Re-Identification Attacks on Health Data. *PLoS ONE*, 6(12), e28071. Online: <http://dx.doi.org/10.1371/journal.pone.0028071>
- Europäische Kommission, 2014. Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), COM 2012(11) final und die konsolidierte Version 2012/0011 (COD), Dokument 11028/14 vom 30. Juni 2014 (deutsche Übersetzung unter <http://www.cr-online.de/DS-GVO-konsolidiert.pdf>, letzter Zugriff 22.10.2012 )
- Frischmann, B.M. (2005). An Economic Theory of Infrastructure and Commons Management”, *Minnesota Law Review*, 89:917-1030.
- Gantz, B. J., & Reinsel, D. (2011). Extracting Value from Chaos State of the Universe : An Executive Summary. *IDC iView*, (June), 1–12. Online: <http://idcdocserv.com/1142>
- Hilbert, M., & López, P. (2011). The world’s technological capacity to store, communicate, and compute information. *Science (New York, N.Y.)*, 332(6025), 60–65. doi:10.1126/science.1200970
- Horvitz, E., & Mulligan, D. (2015). Data, privacy, and the greater good. *Science* , 349 (6245 ), 253–255. doi:10.1126/science.aac4520
- Hsuan, A. B. (Irwin & H. L. (2011). The Cognitive Dissonance of Living in a world of “Big Data.” Retrieved July 2, 2015, from [http://videlectures.net/coinplanetdataschool2011\\_hsuan\\_web/](http://videlectures.net/coinplanetdataschool2011_hsuan_web/)
- Keuper, F., Hamidian, K., Verwaayen, E., Kalinowski, T., & Kraijo, C. (Eds.). (2013). Digitalisierung und Innovation. In *Digitalisierung und Innovation* (p. 504). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-00371-5
- Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity, and Variety. *Application Delivery Strategies*, (February 2001), 2. doi:10.1016/j.infsof.2008.09.005
- Letouzé, E. (2012). *Big Data for Development: Challenges & Opportunities*. *Global Pulse is a United Nations initiative*. Online: <http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf>
- Lycett, M. (2013). Datafication: making sense of (big) data in a complex world. *European Journal of Information Systems*, 22(4), 381–386.

- Manovich, L. (2011). Trending: the promises and the challenges of big social data. In M. K. Gold (Ed.), *Debates in the Digital Humanities*. Minneapolis, MN: The University of Minnesota Press. Retrieved from <http://manovich.net/index.php/projects/trending-the-promises-and-the-challenges-of-big-social-data>
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontier for innovation, competition, and productivity. doi:10.1080/01443610903114527
- McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. (cover story). *Harvard Business Review*, 90(10), 60–68.  
Online: <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=79996279&site=ehost-live>
- Michael, K., & Miller, K. W. (2013). Big Data: New Opportunities and New Challenges [Guest editors' introduction]. *Computer*. doi:10.1109/MC.2013.196
- Mysore, D. (2013). Big data architecture and patterns , Part 2 : How to know if a big data solution is right for your organization, 1–11.
- Naisbitt, J. (1982). *Megatrends: Ten New Directions Transforming Our Lives* (1st ed.). Warner Books, Inc.
- OECD (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264229358-en>
- Page, C., Campbell, R., Coggeshall, S., Gillespie, E., Johnson, R., Olson, M., & Perkins, P. (2012). *Demystifying Big Data: A Practical Guide To Transforming The Business of Government*. Washington, DC. Online: <http://www-04.ibm.com/industries/publicsector/filesolve?contentid=239170>
- Redman, T. C. (2013). Data's Credibility Problem. *Harvard Business Review*, 91(12), 84–88.  
Online: <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=92545713&site=ehost-live>
- Rivers, C. M., & Lewis, B. L. (2014). Ethical research standards in a world of big data [v2; ref status: approved with reservations 2]. *F1000Research*, 3(38). doi:10.12688/f1000research.3-38.v2
- Schroeck, M., Shockley, R., Smart, J., Romero-Morales, D., & Tufano, P. (2012). *Analytics: The real-world use of big data*. IBM Global Business Services Saïd Business School at the University of Oxford. Online: [http://www-03.ibm.com/systems/hu/resources/the\\_real\\_word\\_use\\_of\\_big\\_data.pdf](http://www-03.ibm.com/systems/hu/resources/the_real_word_use_of_big_data.pdf)
- Van Wel, L., & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology*, 6(2), 129–140. doi:10.1023/B:ETIN.0000047476.05912.3d
- Walsh, G., & Möhring, M. (2014). Retourenvermeidung im E-Commerce — Kann Big Data helfen? *Marketing Review St. Gallen*, 31(1), 68–78. doi:10.1365/s11621-014-0322-6
- Winter, R. (2011). *Big Data: Business Opportunities, Requirements and Oracle's Approach*. Cambridge, Massachusetts, USA.
- Zacher, M. (2012). *IDC-Studie: Big Data in Deutschland 2012 – Unternehmen stehen noch ganz am Anfang*. Frankfurt am Main. Retrieved from [http://idc.de/dwn/SF\\_98853/pm17\\_idc\\_studie\\_big\\_data\\_in\\_deutschland\\_2012.pdf](http://idc.de/dwn/SF_98853/pm17_idc_studie_big_data_in_deutschland_2012.pdf)

# Anhang 1: Interview-Leitfaden für „Akteure mit Big Data“

## Schwerpunkt: Daten und Datenzugang

- Was bedeutet für Sie Big Data? Wo sehen Sie die Chancen und Risiken?
- Was ist in Ihrer Organisation die Datenbasis für Big Data? (Bestand, Schwierigkeiten, Vorteile, Nutzen)
- Datenquellen: Werden Daten zugekauft? | durch Kooperation erhalten? | durch Datenaustausch mit Dritten? | Selbst wie akquiriert? | Bezug von staatlichen Daten?
- Datensenzen: Werden Daten weitergegeben? | In kooperative Strukturen eingebracht?
- Haben Sie genug Daten? | ausreichenden Zugang zu Big Data? | im Vergleich mit Konkurrenten / Partnern?
- Qualität der Daten: Kennen Sie die Qualität ihrer Daten? | deren Aktualität? | deren Bezugsrahmen? | den Nutzungsvertrag bei Erhebung? | die Urheberrechte? | Wie stellen Sie diese Aspekte sicher?

## Schwerpunkt: Ethischer Umgang und Reputation

- Wie würde Big Data in einer idealen Welt eingesetzt?
- Gibt es in Ihrer Organisation Richtlinien zum ethisch korrekten Umgang mit Big Data resp. mit Daten generell? Wenn ja, was sind die zentralen Punkte darin?
- Wie wird die Einhaltung solcher Richtlinien überprüft? Wie passt dies zu den internen Anreizsystemen (Boni, etc.)?
- Wie stellt Ihre Organisation sicher, dass die „offline“ Gesetze zum Persönlichkeits- und Datenschutz auch online greifen? (z.B. Recht, Dinge zu verschweigen; Anonymität; Fristen bei der Aktenhaltung, etc.)
- Haben | Kennen Sie Mechanismen wie Kunden Daten einsehen und allfällig korrigieren können?
- Sind bei digitalen Kunden-Identitäten alle Teile gleichermaßen schützenswert?

## Schwerpunkt: Gesellschaftliche Aspekte

- Stellen Sie eine Veränderung des Verhaltens Ihrer Kunden mit einer zunehmenden Gewöhnung an Big Data fest? (Ein steigendes Bewusstsein für „persönliche Daten als Vermögenswert“ könnte bspw. zu einem Preis-Anstieg beim Tausch von „Privacy vs. Service“ führen...)
- Welche Gegenleistungen verwendet Ihre Organisation, um Kunden fürs Erfassen von Daten zu entschädigen? (z.B. Überspringen von Werbung, exklusive Angebote, etc.)
- Braucht es vertrauenswürdige Intermediäre zur Überwachung der Privatsphäre? Wer könnte eine solche Rolle wahrnehmen?
- Wie stellen Sie Transparenz gegenüber den Nutzern her und welche Möglichkeiten zur persönlichen Daten-Kontrolle/Änderung haben diese?

## Schwerpunkt: Innerhalb der Organisation

- Wie ist Big Data innerhalb Ihrer Organisation verankert?
- Welcher Abteilung ist Big Data bei Ihnen zugeordnet?
- Wie viele Stellen-Prozent stehen ausschliesslich für Big Data zur Verfügung? (Wie viele MA hat Ihre Organisation?)
- Wurden durch Big Data bereits organisatorische Anpassungen und Veränderungen angestossen? Wenn ja, welche?
- Welches sind die grössten Schwierigkeiten, Big Data zu valorisieren?

## **Schwerpunkt: Handlungsrichtlinien**

- Welche Richtlinien für die Datennutzung setzt Ihre Organisation heute bereits um?
- Welche Richtlinien wären wünschenswert?
- Wie werden diese überprüft | durchgesetzt?
- Wie bereitet Ihre Organisation sich auf die Einhaltung von zukünftigen Richtlinien für die Datennutzung vor?
- Wie vermitteln Sie dies ihren Kunden?
- Kennen Sie die Datenschutzrichtlinien anderer Organisationen?

## **Schwerpunkt: Technologie**

- Welches sind Ihre zentralen technischen Herausforderungen mit Big Data?
- Welche Herausforderungen ergeben sich für Ihre Organisation daraus, dass es sich bei vielen Big Data Technologien um Open Source Software handelt?

•

## Anhang 2: Interview-Leitfaden für „Beobachter von Big Data“

### Schwerpunkt: Daten und Datenzugang

- Was bedeutet für Sie Big Data? Wo sehen Sie die Chancen und Risiken?
- Welche Branchen profitieren am stärksten von Big Data?
- Welche Chancen entstehen durch die breite Verfügbarkeit von Daten?
- Welche Vorteile bestehen, wenn die Daten nicht verfügbar sind?
- Welche Risiken entstehen durch die breite Verfügbarkeit von Daten?
- Welche Risiken entstehen, wenn die Daten nicht verfügbar sind?

### Schwerpunkt: Ethischer Umgang mit Big Data

- Wie würde Big Data in einer idealen Welt eingesetzt?
- Kennen Sie Richtlinien von Organisationen zum ethisch korrekten Umgang mit Big Data? Wie sehen diese aus? Wie lässt sich deren Einhaltung überprüfen?
- Wie lässt sich sicherstellen, dass die „Offline“-Gesetze zum Persönlichkeits- und Datenschutz auch online bei Organisationen greifen? (z.B. Recht, Dinge zu verschweigen; Anonymität; Fristen bei der Aktenhaltung, etc.)
- Welche Ereignisse gilt es, aus ethischer Sicht auf jeden Fall zu vermeiden?
- Sind alle Teile / Facetten einer digitalen Identität gleichermaßen schützenswert?

### Schwerpunkt: Gesellschaftliche Aspekte

- Lässt sich eine Veränderung des Verhaltens der Konsumenten mit einer zunehmenden Gewöhnung an Big Data feststellen? (Ein steigendes Bewusstsein für „persönliche Daten als Vermögenswert“ könnte bspw. zu einem Preis-Anstieg beim Tausch von „Privacy vs. Service“ führen...)
- Was ist eine angemessene Gegenleistungen beim Tausch von „Privacy vs. Service“? (z.B. Überspringen von Werbung, exklusive Angebote, etc.)
- Braucht es vertrauenswürdige Intermediäre zur Überwachung der Privatsphäre? Wer könnte eine solche Rolle wahrnehmen?

### Schwerpunkt: Wandel der Organisationen

- Wie können Organisationen dazu gebracht werden, Big Data sozial verträglich zu implementieren?

### Schwerpunkt: Handlungsrichtlinien

- Kennen Sie die Datenschutzrichtlinien, denen die Organisationen unterworfen sind, denen Sie Ihre Daten anvertrauen?
- Welche Richtlinien wären wünschenswert?
- Wie sollen diese überprüft werden?

### Schwerpunkt: Technologie

- Wo sehen Sie die zentralen technischen Herausforderungen im Zusammenhang mit Big Data?

## Anhang 3: Fragebogen<sup>26</sup>

### **Big Data: Chancen, Risiken und Handlungsbedarf des Bundes**

Sehr geehrte Damen und Herren,

Die zunehmende Verwendung von Daten in immer mehr Bereichen von Wirtschaft und Gesellschaft birgt viele Chancen, stellt uns aber auch vor etliche neue Herausforderungen. Dabei wird der Trend hin zur Analyse von immer grösseren Datenmengen, zum Zusammenführen von Daten aus ganz unterschiedlichen Quellen und zur immer schnelleren Verarbeitung von Daten gemeinhin unter dem Oberbegriff "Big Data" zusammengefasst.

Angesichts der rasanten Ausbreitung von Big Data setzt sich der Bundesrat im laufenden Jahr mit dieser Thematik auseinander. Vor diesem Hintergrund hat das Bundesamt für Kommunikation die vorliegende Befragung in Auftrag gegeben.

Die Befragung dient dazu, Chancen, Risiken und Handlungsbedarf des Bundes im Zusammenhang mit Big Data aufzuzeigen und aus der Perspektive verschiedener Stakeholdergruppen zu bewerten. Die Ergebnisse der Studie werden bei der zukünftigen Umsetzung der bundesrätlichen Strategie Informationsgesellschaft Schweiz einfließen.

#### **Hinweise zum Ausfüllen des Fragebogens**

- Wo nicht explizit anders vermerkt, interessiert uns Ihre persönliche Einschätzung hinsichtlich der verschiedenen Fragen und nicht die offizielle Position Ihrer Organisation oder Ihres Arbeitgebers.
- Bei vielen Fragen werden Sie nach Ihrer Meinung gefragt, inwieweit ein bestimmter Sachverhalt zutrifft. Dabei gibt es keine "richtige" oder "falsche" Antwort; wählen Sie einfach jene Option, die Ihnen am zutreffendsten erscheint. Falls es Ihnen bei einzelnen Fragen nicht möglich ist, eine sinnvolle Antwort zu geben, wählen Sie bitte die Option "keine Antwort möglich".
- Falls Sie über einen personalisierten Link auf den Fragebogen zugreifen, können Sie das Ausfüllen des Online-Fragebogens jederzeit unterbrechen und zu einem späteren Zeitpunkt fortsetzen. Ihre Daten werden zwischengespeichert.

#### **Datenschutzbestimmungen**

Sämtliche Antworten werden anonym und streng vertraulich behandelt. Ihre Antworten werden weder mit Ihrer Person noch mit Ihrer Organisation / Ihrem Unternehmen verknüpft. Die Angabe Ihrer Kontaktdaten am Ende der Umfrage ist freiwillig. Weder das Forschungsteam noch Dritte werden Sie infolge Ihrer Teilnahme an der Umfrage kontaktieren, wenn Sie dies nicht ausdrücklich wünschen.

Vielen Dank für Ihre Mitarbeit!

Prof. Dr. Thomas Jarchow  
Beat Estermann

<sup>26</sup> Die Befragung fand in Form einer Online-Umfrage statt. Die Informationen bezüglich der Anzeige-Logik sind auf Englisch. Die Erläuterungen wurden in Form von Fussnoten mit dazugehörigen Pop-Up-Fenstern umgesetzt.

Berner Fachhochschule, E-Government-Institut  
**A – Informationen zu Ihrer Person**

**A-1:** Ihr Geschlecht?

- männlich
- weiblich
- keine Antwort

**A-2:** Ihr Alter?

- unter 20 Jahren
- 20 bis 29 Jahre
- 30 bis 39 Jahre
- 40 bis 49 Jahre
- 50 bis 59 Jahre
- 60 bis 69 Jahre
- über 70 Jahre

**A-3:** In welchem Kanton wohnen bzw. arbeiten Sie?

- Wohnkanton: [Drop Down List 1]
- Arbeitskanton: [Drop Down List 2]

[Drop Down List 1/2]

- AG
- AR
- AI
- BE
- BL
- BS
- FR
- GE
- GL
- GR
- JU
- LU
- NE
- NW
- OW
- SG
- SH
- SO
- SZ
- TG
- TI
- UR
- VD
- VS
- ZG
- ZH
- Ich wohne nicht in der Schweiz. [only in Drop Down List 1]
- Ich arbeite nicht in der Schweiz. [only in Drop Down List 2]

**A-4:** Welchen Bezug haben Sie zu Daten?

*Mehrere Antworten möglich. Geben Sie alles Zutreffende an.*

- Ich habe oft beruflich mit Daten zu tun.
- Ich interessiere mich im Rahmen meiner politischen Tätigkeit bzw. meines zivilgesellschaftlichen Engagements für datenbezogene Belange (Open Data, Datenschutz usw.).
- Ich setze mich in meinem Privatleben oft mit den Implikationen einer breiten Nutzung von Daten auseinander.
- Einen anderen Bezug (welchen?):
- Ich habe keinen Bezug zu Daten.

### Display A-5 to A-9 only if the respondent has professional use of data (as indicated in A-4). ###

**A-5:** In welchem Tätigkeitsfeld haben Sie beruflich mit Daten zu tun?

*Mehrere Antworten möglich. Geben Sie alles Zutreffende an.*

- Technik, Informatik
- Marketing, Kommunikation
- Juristische Tätigkeiten
- Forschung und Entwicklung
- Produktion
- Einkauf, Logistik
- Personalwesen
- Administrative Tätigkeiten
- Unterricht, Lehre
- Unternehmensführung, Management
- Anderes Tätigkeitsfeld (welches?):

**A-6:** Welcher Branche gehört Ihr Unternehmen/Ihre Organisation an?

- Landwirtschaft, Gärtnerei, Forstwirtschaft
- Baugewerbe, Bergbau
- Industrie und Gewerbe
- Technik, Informatik, Ingenieurwesen
- Handel, Verkauf
- Transport und Verkehr
- Telekommunikation
- Energie- und Wasserversorgung
- Gastgewerbe, persönliche Dienstleistungen
- Gesundheitswesen, Sozialwesen
- Polizei, Sicherheitswesen
- Banken- und Versicherungswesen
- Informationsdienstleistungen, Kommunikation, Werbung, Marketing
- Management, Administration, Rechtswesen
- Unterrichtswesen, Forschung, Medien, Kultur
- Einer anderen Branche (welcher?):

*Quelle: Adaptiert und erweitert auf der Basis von: CH-X Jugendbefragung 2008/09, Frage 52, sowie anhand der NOGA-Klassifikation.*

**A-7:** Welches ist die Rechtsform Ihres Unternehmens/Ihrer Organisation?

- Öffentlich-rechtliche Organisation
- Privatrechtliche, gemeinnützige Organisation
- Privatrechtliches, gewinnorientiertes Unternehmen
- Andere Rechtsform (welche?):

**A-8:** Wie viele Mitarbeitende zählt Ihr Unternehmen/Ihre Organisation?  
Angaben in Vollzeitäquivalenten (VZÄ)

- 0-9 VZÄ
- 10-49 VZÄ
- 50-250 VZÄ
- Über 250 VZÄ

**A-9:** Welche datenbezogenen Praktiken spielen in Ihrem Unternehmen/Ihrer Organisation eine wichtige Rolle?

**Folgende datenbezogenen Praktiken spielen in meinem Unternehmen/meiner Organisation eine wichtige Rolle:**

	Nein, überhaupt nicht 1	2	3	4	Ja, sehr 5	Keine Antwort möglich
Verarbeitung von grossen Mengen personenbezogener Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verarbeitung von grossen Mengen nicht-personenbezogener Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verknüpfung von heterogenen Datenbeständen aus unterschiedlichen Quellen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rasche Verarbeitung von aktuellen Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erwerb von Daten Dritter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Aufbereitung und Publikation von Daten zuhanden Dritter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anwendung von nicht hypothesengetriebenen Analysemodellen (Mustererkennung)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datengetriebene Optimierung interner Prozesse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datengetriebene Differenzierung von Produkten/Dienstleistungen und Kundensegmenten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datengetriebene Forschung und Entwicklung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datenbasierte Management-Entscheidungen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Weitere (welche?):	<input type="checkbox"/>					
--------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

### Display A-10 only if the respondent has a data-related political or civic engagement (as indicated in A-4). ###

**A-10:** Welche datenbezogenen Aspekte spielen im Rahmen Ihres politischen oder zivilgesellschaftlichen Engagements eine wichtige Rolle?

**Folgende datenbezogenen Aspekte spielen im Rahmen meines politischen oder zivilgesellschaftlichen Engagements eine wichtige Rolle:**

	Nein, überhaupt nicht				Ja, sehr	Keine Antwort möglich
	1	2	3	4	5	
Datenschutz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recht auf informationelle Selbstbestimmung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freier Zugang zu Wissen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freie Weiterverwendung von nicht- personenbezogenen Daten (Open Data)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weiterverwendung von personenbezogenen Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Konsumentenschutz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Förderung von Medien- / IT- / Datenkompetenz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Innovationsförderung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standortförderung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vertretung von Branchen-Interessen (falls ja, welche Branchen?):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weitere (welche?):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## B – Chancen und Risiken von Big Data

**Hinweis:** Unter “Big Data” verstehen wir im Rahmen dieser Umfrage Praktiken, welche sich dadurch kennzeichnen, dass grosse Datenmengen aus sehr unterschiedlichen Quellen zusammengeführt und – oftmals sehr zeitnah – analysiert und ausgewertet werden.

**B-1:** Welches sind aus Ihrer Sicht die wichtigsten Chancen von Big Data?

**Aus meiner Sicht ist Big Data ein wichtiges Mittel, ...**

*Bitte bewerten Sie die Chancen von Big Data unabhängig davon, ob Sie die jeweilige Entwicklung gut oder schlecht finden.*

	Nein, überhaupt nicht				Ja, sehr	Keine Antwort möglich
	1	2	3	4	5	
um neue Zusammenhänge zu entdecken / neue Erkenntnisse zu gewinnen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um die Personalisierung von Informationen und Dienstleistungen zu ermöglichen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um personalisierte Werbung zu ermöglichen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um intelligente, individualisierte Preismodelle zu ermöglichen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um “Schwarze Schafe” unter den Wirtschaftsakteuren (z.B. schlechte Zahler) frühzeitig zu identifizieren	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um genauere Prognosen und Risikoabschätzungen zu ermöglichen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um operative und logistische Abläufe optimieren zu können	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um Unternehmen und Organisationen ein agileres Handeln zu ermöglichen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
um ein Daten- und Fakten-basiertes Handeln zu fördern	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weitere (welche?):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**B-2: Welches sind aus Ihrer Sicht die bedeutendsten Risiken im Zusammenhang mit Big Data?**

**Aus meiner Sicht sind dies bedeutende Risiken von Big Data:**

	Nein, überhaupt nicht				Ja, sehr	Keine Antwort möglich
	1	2	3	4	5	
Grundsätzliche Bedrohung der Privatsphäre	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Missbräuchliche Verwendung der Daten / Datendiebstahl	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erhöhte Gefahr von ökonomischer Diskriminierung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erhöhte Gefahr von staatlicher Repression	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erhöhte Gefahr von persönlicher Repression (Stalking, Mobbing, Identitätsdiebstahl u.ä.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erhöhte Gefahr von politischer Manipulation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erhöhte Gefahr von Betrugs- und Täuschungsdelikten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unkontrollierte Eigendynamik der Systeme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verschärfung von politischen und ökonomischen Machtgefällen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zu starke Fokussierung auf Daten bei der Entscheidungsfindung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weitere (welche?):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### The items of B-3 are displayed according to the information provided in A-4. Item 1 is displayed to all respondents; items 2 and 3 to respondents with a professional activity related to data; and item 4 to respondents with political / civic engagement related to data.  
###

**B-3: Wie beurteilen Sie die Chancen und Risiken von Big Data?**

	Die Risiken überwiegen deutlich				Die Chancen überwiegen deutlich	Keine Antwort möglich
	1	2	3	4	5	
Für Sie persönlich?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Aus Sicht Ihres Arbeitgebers (Unternehmen/Organisation)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Aus Sicht Ihrer Branche?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Aus Sicht Ihres politischen / zivilgesellschaftlichen Engagements	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Hinweis:** Unter “kollektivem Handlungsbedarf” verstehen wir im Rahmen dieser Umfrage einen Bedarf nach gesellschaftlich abgestimmtem Vorgehen, wobei offen ist, inwieweit die Koordination durch den Staat, die Privatwirtschaft oder durch zivilgesellschaftliche Akteure erfolgen soll.

**Hinweis:** Als “Open Data” werden Daten bezeichnet, die im Internet in einem maschinenlesbaren Format frei verfügbar gemacht werden, so dass sie von jedermann für beliebige Zwecke verwendet, modifiziert und weiterverbreitet werden können (einschliesslich der kommerziellen Nutzung). Von der Anwendung des Open-Data-Prinzips nicht betroffen sind in der Regel personenbezogene Daten, sicherheitsrelevante Daten sowie Daten, die der Geheimhaltung unterliegen.

**B-4: In welchen Bereichen sehen Sie kollektiven Handlungsbedarf, um sicherzustellen, dass die positiven Seiten von Big Data zum Tragen kommen?**

**In den folgenden Bereichen sehe ich...**

	keinen Handlungs- bedarf				sehr grossen Handlungs- bedarf	keine Antwort möglich
	1	2	3	4	5	
Abbau datenschutzrechtlicher Hürden für Unternehmen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Standardisierung von technischen Schnittstellen	<input type="checkbox"/>					
Vergabe von Datenschutzlabels im Rahmen einer Zertifizierung von Unternehmen/Organisationen	<input type="checkbox"/>					
Bereitstellung von Diensten, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen	<input type="checkbox"/>					
Konsequente Umsetzung des Open-Data-Prinzips in der öffentlichen Verwaltung	<input type="checkbox"/>					
Konsequente Umsetzung des Open-Data-Prinzips im Bereich der Forschung	<input type="checkbox"/>					
Konsequente Umsetzung des Open-Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor)	<input type="checkbox"/>					
Schaffen von Mechanismen, welche es dem Einzelnen erlauben, seine personenbezogenen Daten – unter Beibehaltung grösstmöglicher Kontrolle – für die Weiterverwendung durch Dritte freizugeben (z.B. im Gesundheitsbereich)	<input type="checkbox"/>					
Förderung der Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.)	<input type="checkbox"/>					
Förderung der Forschung im Bereich künstliche Intelligenz	<input type="checkbox"/>					
Förderung der Sekundärnutzung von Daten innerhalb der öffentlichen Verwaltung  <b>Hinweis:</b> “Sekundärnutzung” bezeichnet die Weiterverwendung der Daten über den ursprünglichen Erhebungs- und Nutzungskontext hinaus.”	<input type="checkbox"/>					
Förderung der Sekundärnutzung von Daten in der Forschung	<input type="checkbox"/>					
Förderung der Sekundärnutzung von Daten durch die Privatwirtschaft	<input type="checkbox"/>					
Bereitstellung der technischen Infrastruktur für die Bereitstellung und Archivierung von sehr grossen Datenmengen	<input type="checkbox"/>					
Weitere (welche?):	<input type="checkbox"/>					

**B-5: In welchen Bereichen sehen Sie kollektiven Handlungsbedarf, um sicherzustellen, dass die Risiken von Big Data minimiert werden?**

**In den folgenden Bereichen sehe ich...**

	keinen Handlungsbedarf				sehr grossen Handlungsbedarf	keine Antwort möglich
	1	2	3	4	5	
Definition von neuen Eigentums- oder Nutzungsrechten im Bereich der personenbezogenen Daten	<input type="checkbox"/>	<input type="checkbox"/>				
Verschärfung der Datenschutzregeln für die Privatwirtschaft	<input type="checkbox"/>	<input type="checkbox"/>				
Verschärfung der Datenschutzregeln für die Forschung	<input type="checkbox"/>	<input type="checkbox"/>				
Verschärfung der Datenschutzregeln für Behörden	<input type="checkbox"/>	<input type="checkbox"/>				
Zertifizierung von Unternehmen und Vergabe von Datenschutzlabels zur Durchsetzung höherer Datenschutzstandards am Markt	<input type="checkbox"/>	<input type="checkbox"/>				
Verbesserung des Schutzes von Whistleblowern / Förderung des investigativen Journalismus	<input type="checkbox"/>	<input type="checkbox"/>				
Erweiterte Kompetenzen für Datenschutzbeauftragte	<input type="checkbox"/>	<input type="checkbox"/>				
Verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich	<input type="checkbox"/>	<input type="checkbox"/>				
Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes	<input type="checkbox"/>	<input type="checkbox"/>				
Förderung der Entwicklung von Lösungen zur Verbesserung der Human-Data-Interaktion	<input type="checkbox"/>	<input type="checkbox"/>				
Aufklärungs- und Sensibilisierungsmassnahmen	<input type="checkbox"/>	<input type="checkbox"/>				
Weitere (welche?):	<input type="checkbox"/>	<input type="checkbox"/>				

## C – Datenschutz und Data Governance

**C-1:** Hinsichtlich der künftigen Ausgestaltung des Datenschutzes gibt es unterschiedliche Vorstellungen. Inwieweit treffen die untenstehenden Aussagen aus Ihrer Sicht zu?

**Die Aussage trifft aus meiner Sicht...**

### Display items in randomized order. ###

	überhaupt nicht zu				vollkommen zu	keine Antwort möglich
	1	2	3	4	5	
Besonders zu schützen sind Daten zu Gesundheit, finanzieller Situation, Religion, politischer Zugehörigkeit u.ä.	<input type="checkbox"/>					
Nicht besonders zu schützen sind Daten, die sowieso öffentlich sind, wie Name, Wohnort, Alter, Geschlecht.	<input type="checkbox"/>					
Besonders zu schützen sind Daten, die es erlauben, jemanden zu identifizieren.	<input type="checkbox"/>					
Besonders problematisch ist das Verbinden von Personendaten aus verschiedenen Quellen in einem Personenprofil.	<input type="checkbox"/>					
Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt.	<input type="checkbox"/>					
Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Daten ist nicht sinnvoll; die Frage, welche Daten schützenswert sind, muss kontextabhängig beantwortet werden.	<input type="checkbox"/>					
Es sollte in der Kontrolle jeder/jedes Einzelnen liegen, welche Daten er/sie wem zu welchem Zweck preisgeben möchte.	<input type="checkbox"/>					
Die digitale Identität gilt es gleich zu schützen wie die physische; analog zur Garantie der physischen Unversehrtheit müssen auch die Daten, die einen betreffen, korrekt sein.	<input type="checkbox"/>					

**C-2:** Hinsichtlich der Ausrichtung der künftigen Data-Governance gibt es unterschiedliche Vorstellungen. Inwieweit halten Sie die untenstehenden Maximen angesichts Ihrer persönlichen Situation und jener Ihres persönlichen Umfeldes für sinnvoll?

**Angesichts meiner persönlichen Situation und jener meines persönlichen Umfeldes erscheinen die folgenden Maximen als...**

### Display items in randomized order. ###

	überhaupt nicht sinnvoll				äusserst sinnvoll	keine Antwort möglich
	1	2	3	4	5	
Jede(r) Einzelne soll die Herrschaft über die ihn/sie betreffenden personenbezogenen Daten ausüben.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Der Datenschutz ist durch juristische und ökonomische Massnahmen sicherzustellen (Auflagen, Inspektionen, Bussen).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Der Datenschutz ist durch technische Massnahmen sicherzustellen.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ein Maximum an Daten soll im Internet zur allgemeinen Weiterverwendung bereitgestellt werden.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Der Staat muss die Geschäftspraktiken der grossen, internationalen Firmen im Internetbereich stärker regulieren und kontrollieren.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Der Staat muss Massnahmen ergreifen, damit der Markt im Bereich der Daten besser funktioniert.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Im Bereich der Daten spielt der Markt recht gut; der Staat sollte sich heraushalten.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Die Datenschutzproblematik ist durch ein Empowerment der Nutzer / Kunden / Bürgerinnen zu entschärfen.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Conditional question: C-3 is displayed only to respondents with a data-related professional activity. Same items as in C-2. ###

**C-3:** Versetzen Sie sich nun in die Situation Ihres Arbeitgebers (Unternehmen/Organisation).

**Aus der Perspektive meines Unternehmens / meiner Organisation erscheinen die folgenden Maximen als...**

	überhaupt nicht sinnvoll				äusserst sinnvoll	keine Antwort möglich
	1	2	3	4	5	
Same items as in C-2...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Conditional question: C-4 is displayed only to respondents with a data-related political or civic engagement. Same items as in C-2. ###

**C-4:** Beurteilen Sie nun dieselben Maximen aus der Perspektive Ihres politischen bzw. zivilgesellschaftlichen Engagements.

**Aus der Perspektive meines politischen bzw. zivilgesellschaftlichen Engagements erscheinen die folgenden Maximen als...**

	überhaupt nicht zielführend				ganz klar zielführend	keine Antwort möglich
	1	2	3	4	5	
Same items as in C-2...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	<input type="checkbox"/>					
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

**C-5: Der Wert von Daten und die Preisbildung am Daten-Markt** wird von verschiedenen Menschen unterschiedlich bewertet. Inwieweit treffen die untenstehenden Aussagen aus Ihrer Sicht zu?

**Die Aussage trifft aus meiner Sicht...**

### Display items in randomized order. ###

	überhaupt nicht zu				vollkommen zu	keine Antwort möglich
	1	2	3	4	5	
Generell erhalten die Leute für die Preisgabe ihrer Daten im Internet eine faire Gegenleistung.	<input type="checkbox"/>					
Generell erhalten die Leute für die Preisgabe ihrer Daten ausserhalb des Internets eine faire Gegenleistung.	<input type="checkbox"/>					
Es ist aus gesellschaftlicher Sicht problematisch, wenn zu viele Menschen ihre persönlichen Daten aus individuellen Nutzenüberlegungen heraus preisgeben.	<input type="checkbox"/>					
Natürliche Monopole (Netzwerkeffekte) führen dazu, dass der Daten-Markt in etlichen Bereichen versagt.	<input type="checkbox"/>					
Informations-Asymmetrien führen dazu, dass der Datenmarkt in etlichen Bereichen versagt.	<input type="checkbox"/>					
Kunden/Nutzer sind nicht in der Lage, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen.	<input type="checkbox"/>					

## D – Handlungsbedarf der öffentlichen Hand

**D-1:** In Abschnitt B haben Sie in verschiedenen Bereichen kollektiven Handlungsbedarf identifiziert, um sicherzustellen, dass die positiven Seiten von Big Data zum Tragen kommen bzw. die Risiken minimiert werden.

**Geben Sie bitte für jeden der Bereiche an, ob aus Ihrer Sicht in erster Linie der Staat, die Zivilgesellschaft oder die Privatwirtschaft konkret aktiv werden sollte.**

*Mehrere Antworten möglich. Bitte alles Zutreffende ankreuzen.*

### Conditional question: In D-1 the items from B-4 and B-5 are displayed which scored higher than 3 ###

### Massnahmen, um die positiven Seiten von Big Data zu fördern:

	Staat	Privatwirtschaft	Zivilgesellschaft	keine Antwort möglich
Same items as in B-4...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Massnahmen, um die Risiken von Big Data zu minimieren:

	Staat	Privatwirtschaft	Zivilgesellschaft	keine Antwort möglich
Same items as in B-5...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Im untenstehenden Feld können Sie Ihre Angaben bei Bedarf weiter präzisieren:

--

### Conditional question: In D-2 the items from B-4 and B-5 are displayed which scored higher than 3 ###

**D-2:** Geben Sie nun bitte für dieselben Bereiche an, auf welcher Ebene (kantonal/regional, schweizweit, europaweit, weltweit) die entsprechenden Massnahmen koordiniert werden sollten, um erfolgreich zu sein.

*Mehrere Antworten möglich. Bitte alles Zutreffende ankreuzen.*

**Massnahmen, um die positiven Seiten von Big Data zu fördern:**

	kantonal / regional	schweizweit	europaweit	weltweit	keine Antwort möglich
Same items as in B-4...	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				

**Massnahmen, um die Risiken von Big Data zu minimieren:**

	kantonal / regional	schweizweit	europaweit	weltweit	keine Antwort möglich
Same items as in B-5...	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				
	<input type="checkbox"/>				

Im untenstehenden Feld können Sie Ihre Angaben bei Bedarf weiter präzisieren:

--

Damit sind Sie am Ende des Fragebogens angelangt. Wir möchten uns herzlich für Ihre Teilnahme an der Befragung bedanken. Im untenstehenden Feld können Sie Bemerkungen und Kommentare hinterlassen. Falls Sie möchten, dass wir Sie über die weiteren Aktivitäten im Hinblick auf die Entwicklung der neuen Strategie Informationsgesellschaft Schweiz auf dem Laufenden halten, können Sie uns zudem Ihre Kontaktdaten angeben.

*Um die Anonymität der Umfrage zu gewährleisten, werden Ihre im Rahmen des Fragebogens gegebenen Antworten selbstverständlich unabhängig von Ihren Kontaktdaten ausgewertet.*

Bemerkungen / Kommentare:

Bitte halten Sie mich über die weiteren Aktivitäten im Hinblick auf die Entwicklung der neuen Strategie Informationsgesellschaft Schweiz auf dem Laufenden:

*Die Angabe Ihrer Kontaktdaten ist freiwillig; geben Sie diese nur an, falls Sie vom Bundesamt für Kommunikation kontaktiert werden möchten. Falls Sie Ihre Kontaktdaten nicht im Rahmen der Umfrage angeben möchten, können Sie sich bei Interesse an weiteren Informationen auch direkt per E-Mail ans Bundesamt für Kommunikation wenden ([infosociety@bakom.admin.ch](mailto:infosociety@bakom.admin.ch)).*

Nachname:

Vorname:

Organisation (*fakultativ*):

Bevorzugte Sprache:

- Deutsch
- Französisch
- Italienisch

E-Mail:

**Vielen Dank für Ihre Teilnahme an unserer Umfrage!**

Die Umfrageergebnisse werden in die zukünftige Umsetzung der bundesrätlichen Strategie für eine Informationsgesellschaft einfließen. Die Strategie ist publiziert unter: [www.infosociety.ch](http://www.infosociety.ch)

## Anhang 4: Rücklaufquoten der verschiedenen Kategorien von Umfrageteilnehmern

Um sicherzustellen, dass Personen mit unterschiedlichem Hintergrund in die Befragung mit einbezogen werden, wurden die direkt angeschriebenen Personen nach Möglichkeit einer von 12 Kategorien zugeteilt (siehe Tabelle 17). Aufgrund von multiplen Zugehörigkeiten (z.B. Mitarbeiter des Bundes und Mitglied des priorisierten Vorhabens „Open Government Data“) ist diese Zuordnung nicht absolut exakt; sie erlaubt jedoch einen Überblick darüber, welche Personengruppen in welchem Umfang zur Teilnahme an der Umfrage eingeladen wurden, und erlaubt es, die Rücklaufquote auf die einzelnen Teilnehmer-Kategorien aufzuschlüsseln. Hier fällt auf, dass die Gruppe der Personen, welche sich mit dem Schutz von Personendaten auseinandersetzen, und jene der Personen, die mit Open Data zu tun haben, mit 59% bzw. 44% die höchsten Rücklaufquoten aufweisen. Die niedrigste Rücklaufquote erzielten dagegen mit 9% die Medienschaffenden. Alle übrigen Teilnehmer-Kategorien bewegen sich mit Rücklaufquoten zwischen 21% und 35% im Mittelfeld.

Teilnehmer-Kategorie	Anzahl kontaktierte Personen	Anzahl Umfrage-Teilnehmende	Rücklaufquote
Bund	546	155	28%
Kantone	434	151	35%
Städte / Gemeinden	238	49	21%
Gesundheitswesen	51	15	29%
Hochschulen	190	58	31%
Privatwirtschaft	1014	216	21%
Verbände	43	11	26%
Datenschutz	22	13	59%
Open Data	149	66	44%
Politik	60	16	27%
Medienschaffende	35	3	9%
Privatpersonen	53	11	21%
<b>Total direkt Kontaktierte</b>	<b>2838</b>	<b>764</b>	<b>27%</b>
<b>Total Teilnehmende via „Open Call“</b>	-	<b>57</b>	-

Tabelle 17: Rücklaufquoten der verschiedenen Kategorien von Umfrageteilnehmenden

## Anhang 5: Liste sämtlicher Massnahmen

Die untenstehende Tabelle enthält die Liste sämtlicher Massnahmen, zu denen die Umfrageteilnehmer befragt wurden. Für jede Massnahme werden die Zustimmungsrate und die Ablehnungsrate angegeben. Diese geben Auskunft darüber, inwieweit eine Massnahme von den Befragten als wünschenswert betrachtet wird. Dem Diagramm kann zudem entnommen werden, bei welchem Akteur (Staat, Privatwirtschaft und/oder Zivilgesellschaft) die Zuständigkeit verortet wird und auf welcher Ebene bzw. auf welchen Ebenen (kantonal, schweizweit, europaweit und/oder weltweit) die Koordination erfolgen sollte. Hierzu wurden nur die Umfrageteilnehmenden befragt, welche angegeben hatten, dass sie im betreffenden Bereich kollektiven Handlungsbedarf verorten. Aus diesem Grund variiert die Stichprobengrösse (N) zwischen den einzelnen Massnahmen.

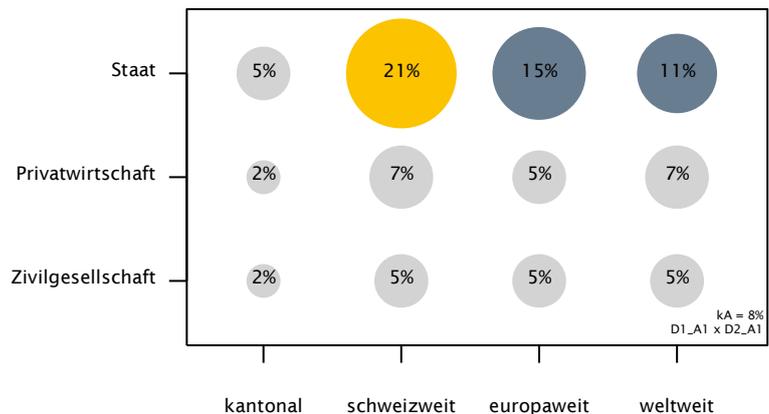
### Abbau datenschutzrechtlicher

#### Hürden für Unternehmen

Zustimmung: 21.5% (N = 168)

Neutrale: 22.2% (N = 173)

Ablehnung: 56.3% (N = 439)

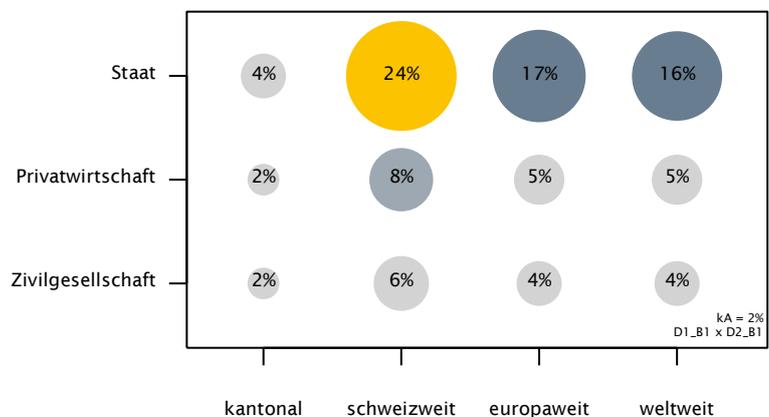


### Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren

Zustimmung: 68.5% (N = 539)

Neutrale: 21.2% (N = 167)

Ablehnung: 10.3% (N = 81)

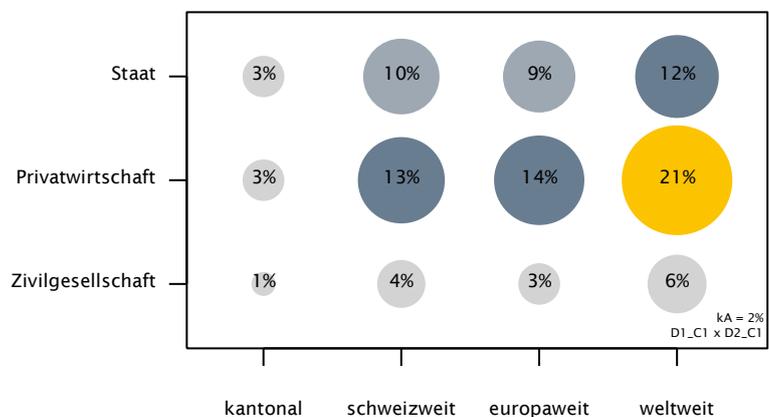


### Standardisierung von technischen Schnittstellen

Zustimmung: 69.1% (N = 542)

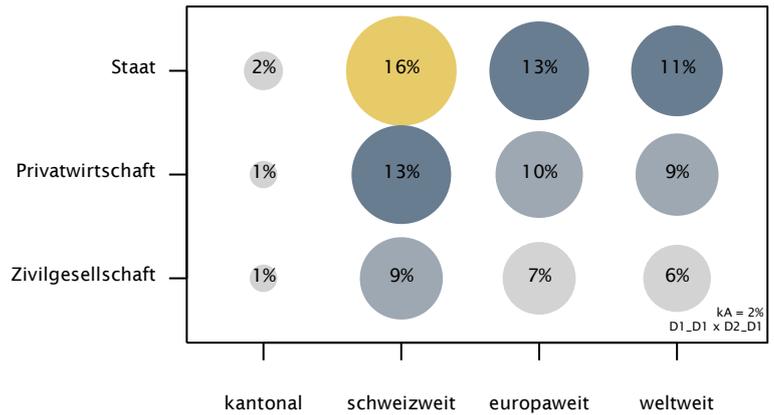
Neutrale: 22.3% (N = 175)

Ablehnung: 8.5% (N = 67)



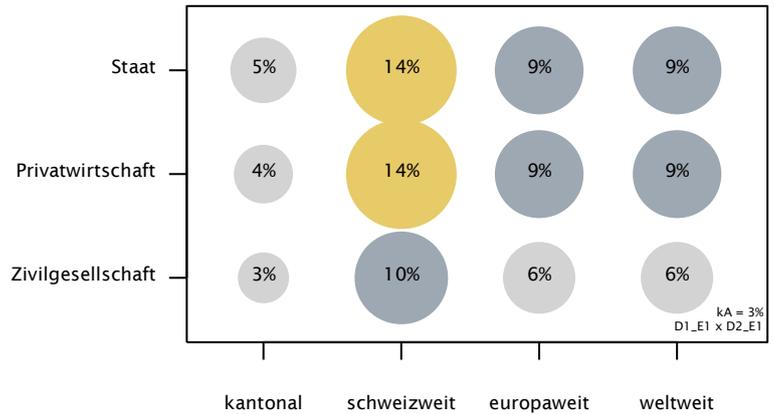
**Vergabe von Datenschutzlabels im Rahmen einer Zertifizierung von Unternehmen/Organisationen**

Zustimmung: 57.5% (N = 458)  
 Neutrale: 23.5% (N = 187)  
 Ablehnung: 19% (N = 151)



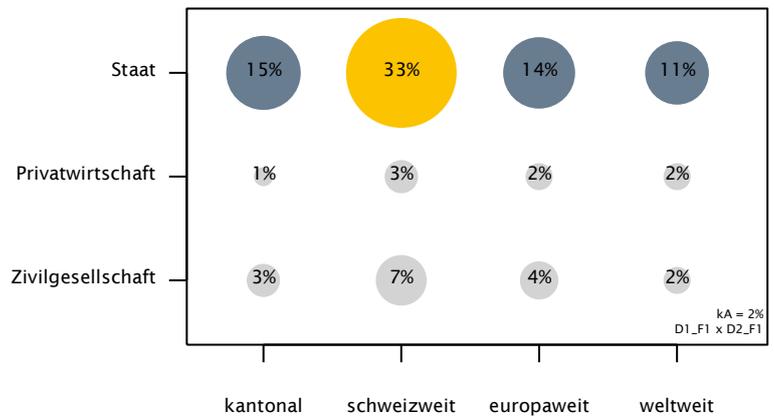
**Bereitstellung von Diensten, die es den Einzelnen erlauben, ihre datenbezogenen Interessen effektiv wahrzunehmen**

Zustimmung: 67.2% (N = 526)  
 Neutrale: 20.9% (N = 164)  
 Ablehnung: 11.9% (N = 93)



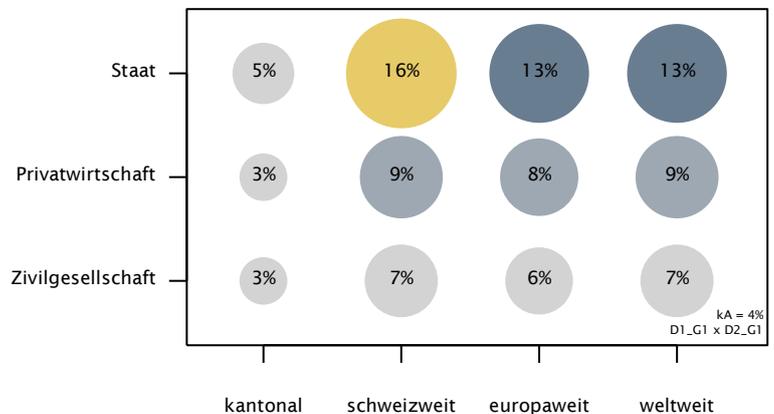
**Konsequente Umsetzung des Hinweis auf Open Data**

Zustimmung: 61.4% (N = 486)  
 Neutrale: 22.9% (N = 181)  
 Ablehnung: 15.8% (N = 125)



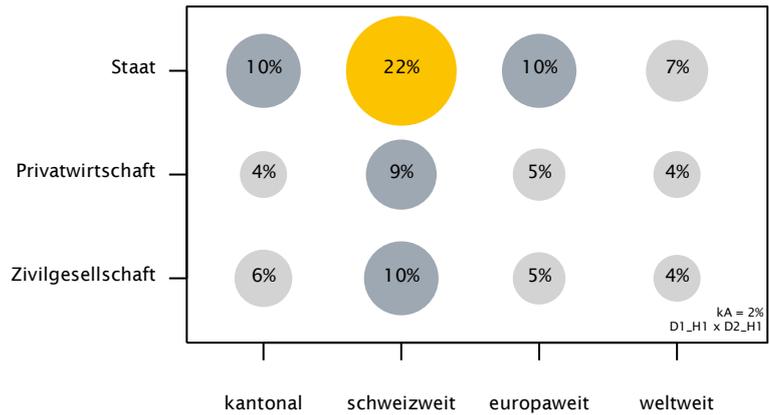
**Konsequente Umsetzung des Open Data-Prinzips im Bereich der Forschung**

Zustimmung: 66.1% (N = 516)  
 Neutrale: 19.6% (N = 153)  
 Ablehnung: 14.3% (N = 112)



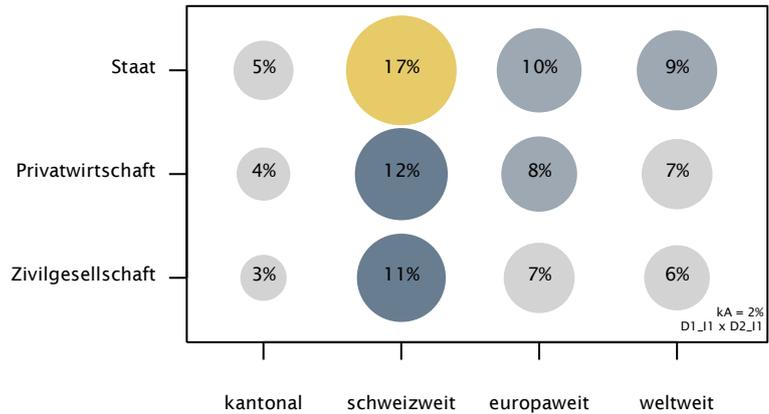
**Konsequente Umsetzung des Open Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor)**

Zustimmung: 55.5% (N = 435)  
 Neutrale: 24.4% (N = 191)  
 Ablehnung: 20.2% (N = 158)



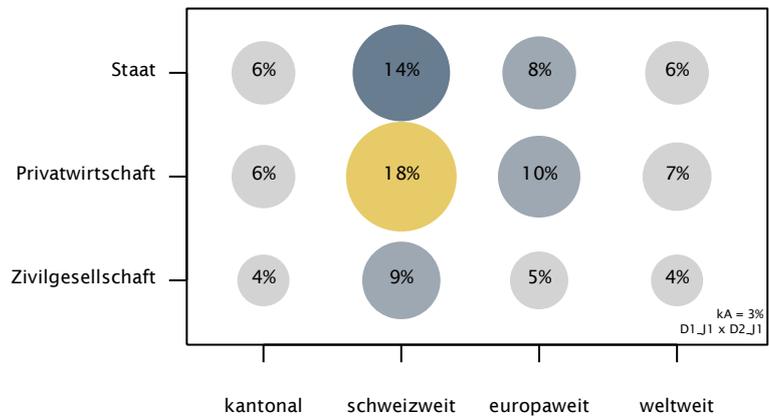
**Schaffen von Mechanismen, welche es dem Einzelnen erlauben, seine personenbezogenen Daten - unter Beibehaltung grösstmöglicher Kontrolle - für die Weiterverwendung durch Dritte freizugeben (z.B. im Gesundheitsbereich)**

Zustimmung: 67.5% (N = 545)  
 Neutrale: 18.5% (N = 149)  
 Ablehnung: 14% (N = 113)



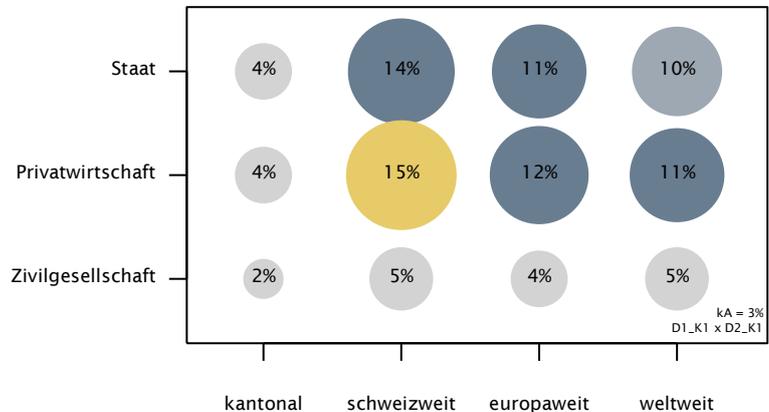
**Förderung der Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.)**

Zustimmung: 64.2% (N = 512)  
 Neutrale: 22.8% (N = 182)  
 Ablehnung: 12.9% (N = 103)



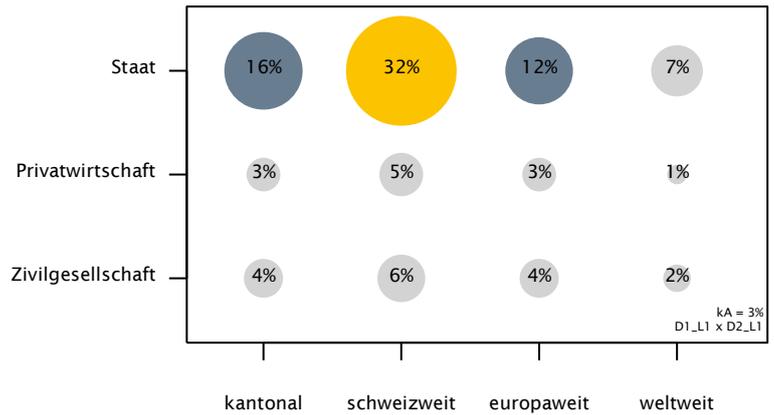
**Förderung der Forschung im Bereich künstliche Intelligenz**

Zustimmung: 41.3% (N = 323)  
 Neutrale: 28.7% (N = 225)  
 Ablehnung: 30% (N = 235)



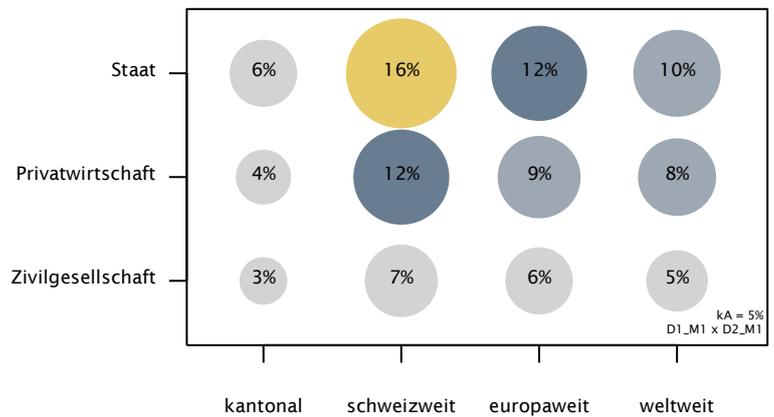
**Förderung der Sekundärnutzung von Daten innerhalb der öffentlichen Verwaltung**

Zustimmung: 47.7% (N = 376)  
 Neutrale: 25.2% (N = 199)  
 Ablehnung: 27.1% (N = 214)



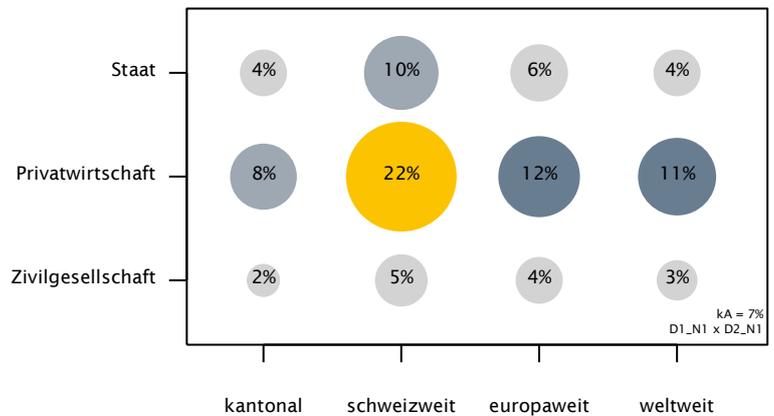
**Förderung der Sekundärnutzung von Daten in der Forschung**

Zustimmung: 53.7% (N = 411)  
 Neutrale: 26.2% (N = 201)  
 Ablehnung: 20.1% (N = 154)



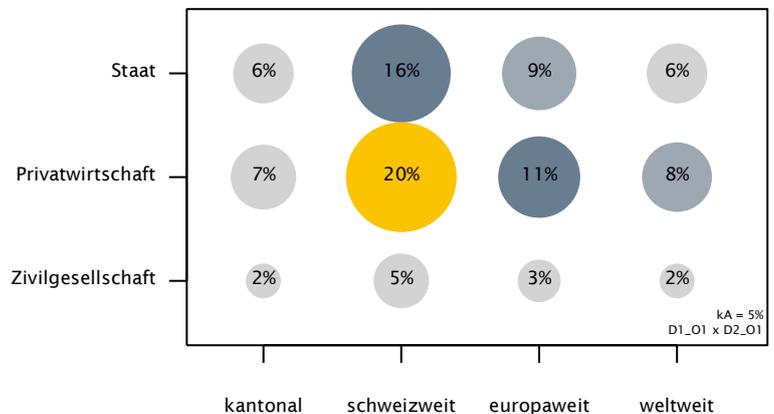
**Förderung der Sekundärnutzung von Daten durch die Privatwirtschaft**

Zustimmung: 32.5% (N = 252)  
 Neutrale: 26.2% (N = 203)  
 Ablehnung: 41.3% (N = 320)



**Bereitstellung der technischen Infrastruktur für die Bereitstellung und Archivierung von sehr grossen Datenmengen**

Zustimmung: 52.8% (N = 417)  
 Neutrale: 22.8% (N = 180)  
 Ablehnung: 24.4% (N = 193)

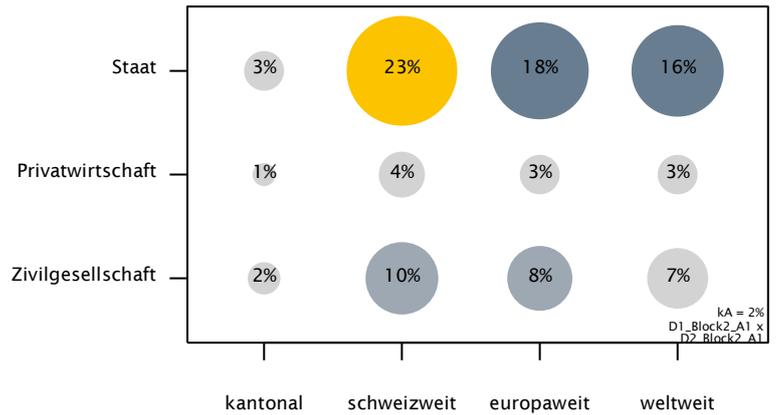


**Definition von neuen Eigentums- oder Nutzungs-rechten im Bereich der personenbezogenen Daten**

Zustimmung: 75.1% (N = 604)

Neutrale: 14.8% (N = 119)

Ablehnung: 10.1% (N = 81)

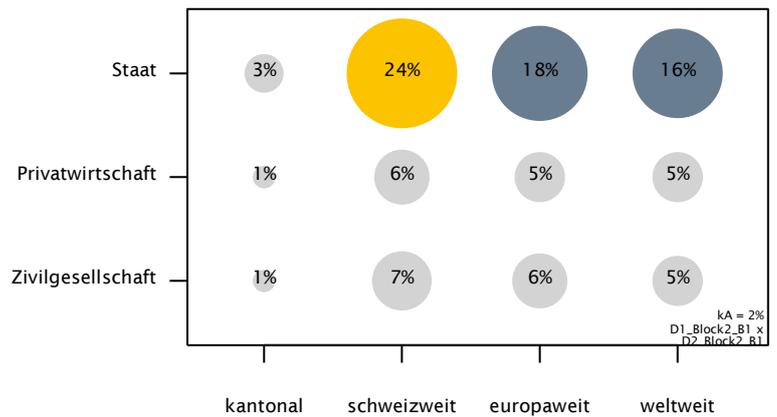


**Verschärfung der Datenschutz-regeln für die Privatwirtschaft**

Zustimmung: 61.1% (N = 490)

Neutrale: 20.4% (N = 164)

Ablehnung: 18.5% (N = 148)

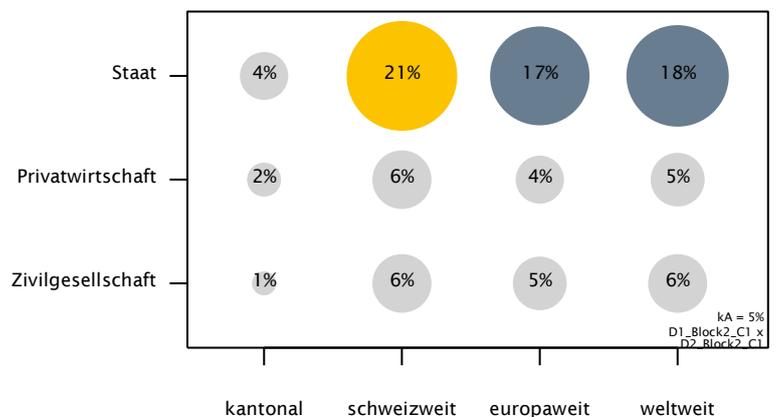


**Verschärfung der Datenschutz-regeln für die Forschung**

Zustimmung: 35.2% (N = 277)

Neutrale: 30.7% (N = 242)

Ablehnung: 34.1% (N = 269)

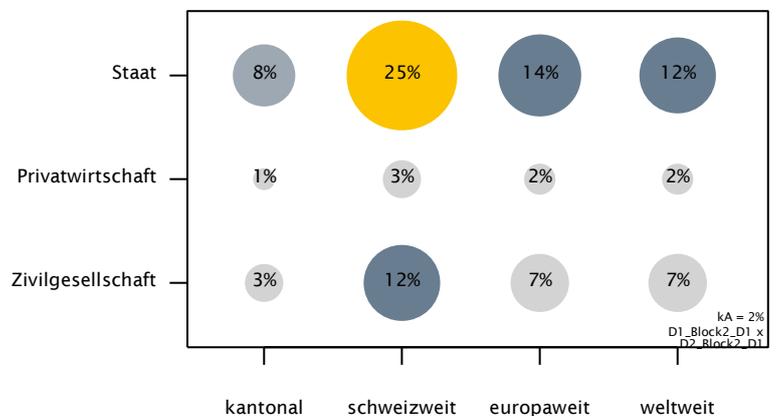


**Verschärfung der Datenschutz-regeln für Behörden**

Zustimmung: 39.6% (N = 318)

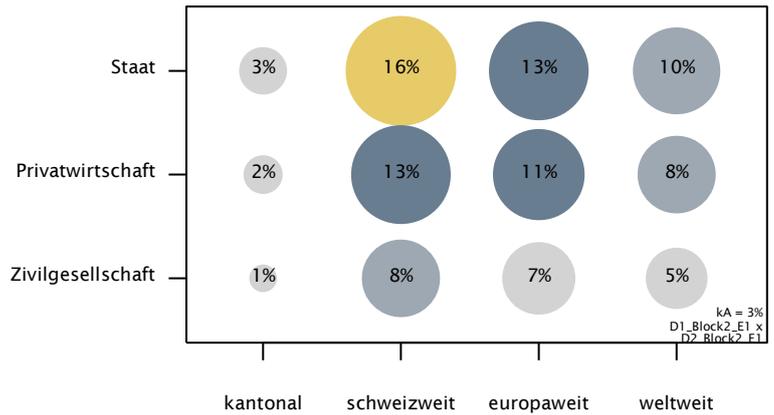
Neutrale: 27.6% (N = 222)

Ablehnung: 32.8% (N = 263)



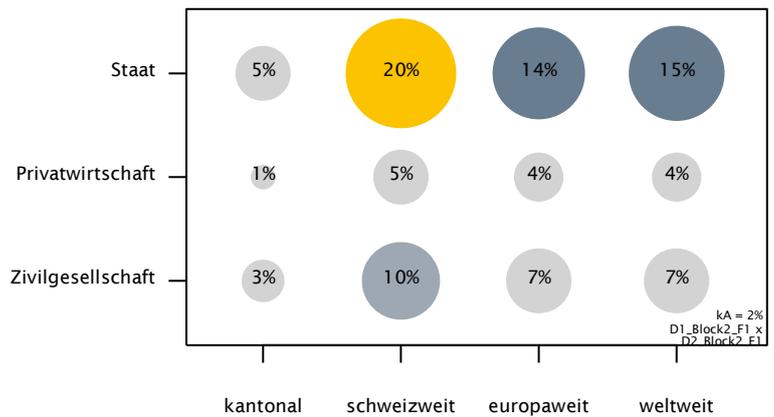
**Zertifizierung von Unternehmen und Vergabe von Datenschutzlabels zur Durchsetzung höherer Datenschutzstandards am Markt**

Zustimmung: 56% (N = 446)  
 Neutrale: 25.3% (N = 201)  
 Ablehnung: 18.7% (N = 149)



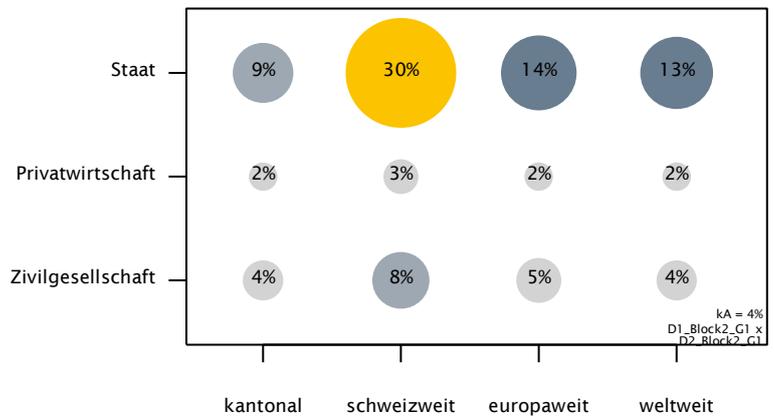
**Verbesserung des Schutzes von Whistleblowern / Förderung des investigativen Journalismus**

Zustimmung: 53.3% (N = 426)  
 Neutrale: 24.8% (N = 198)  
 Ablehnung: 21.9% (N = 175)



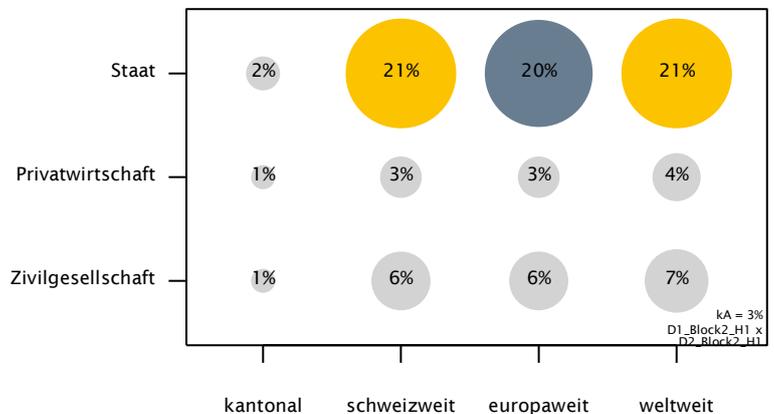
**Erweiterte Kompetenzen für Datenschützer**

Zustimmung: 50.2% (N = 403)  
 Neutrale: 23.7% (N = 190)  
 Ablehnung: 26.2% (N = 210)



**Verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-) Monopolisten im Internet-Bereich**

Zustimmung: 63.9% (N = 507)  
 Neutrale: 22.4% (N = 178)  
 Ablehnung: 13.6% (N = 108)

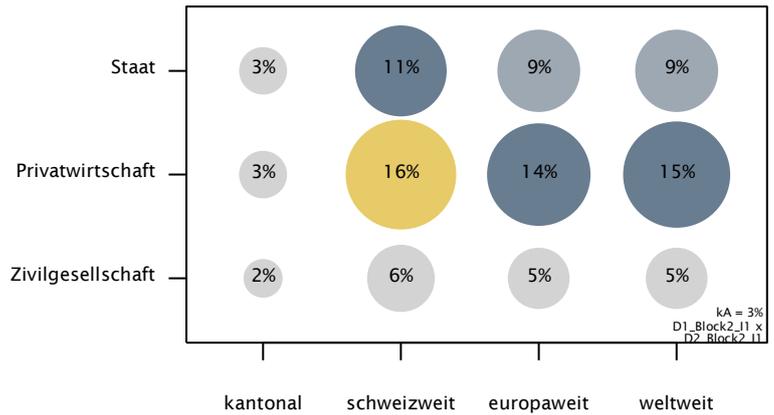


**Förderung der Entwicklung von technischen Lösungen zur Sicherstellung des Datenschutzes**

Zustimmung: 73.1% (N = 591)

Neutrale: 17.9% (N = 145)

Ablehnung: 8.9% (N = 72)



**Förderung der Entwicklung von Lösungen zur Verbesserung der Human-Data-Interaction**

Zustimmung: 55.2% (N = 406)

Neutrale: 30.1% (N = 221)

Ablehnung: 14.7% (N = 108)

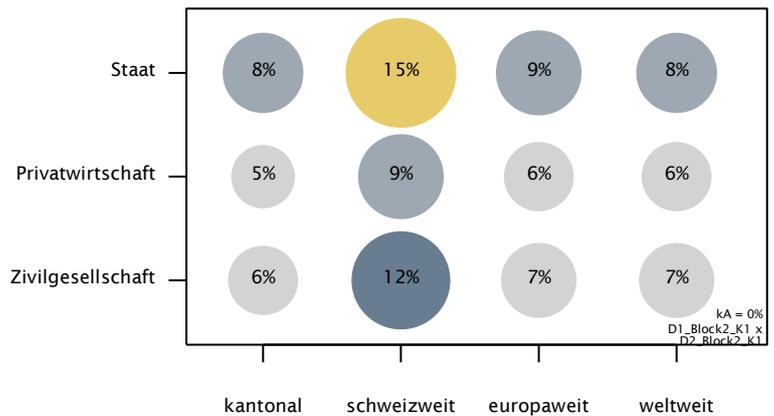


**Aufklärungs- und Sensibilisierungsmassnahmen**

Zustimmung: 71.9% (N = 581)

Neutrale: 20.4% (N = 165)

Ablehnung: 7.7% (N = 62)



## Anhang 6: Analyse der Abschnitte B und C des Fragebogens

Bei den Fragen der Abschnitte B und C des Fragebogens wurden anhand von Hauptkomponentenanalysen die verschiedenen Dimensionen eruiert und die dazugehörigen Werte (scores) ermittelt. Die nachfolgenden Tabellen enthalten die jeweiligen Dimensionen (Faktoren), die dazugehörigen Fragebogen-Items, Cronbachs Alpha<sup>27</sup> sowie den Anteil positiver Antworten für die jeweilige Dimension, d.h. den Anteil Befragter, welche für die jeweilige Dimension auf einer Skala von 1 bis 5 einen Wert (score) von über 3 Punkten aufweisen.

Die Fragen B1 und B2 beziehen sich auf die verschiedenen **Auswirkungen von Big Data**:

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Big Data erhöht die Gefahr von Manipulation</b>	<ul style="list-style-type: none"> <li>• Verschärfung von politischen und ökonomischen Machtgefällen</li> <li>• Erhöhte Gefahr von politischer Manipulation</li> <li>• Zu starke Fokussierung auf Daten bei der Entscheidungsfindung</li> <li>• Unkontrollierte Eigendynamik der Systeme</li> <li>• Erhöhte Gefahr von ökonomischer Diskriminierung</li> <li>• Erhöhte Gefahr von staatlicher Repression</li> </ul>	0.818	67%
<b>Big Data bedroht die Privatsphäre und erhöht die Gefahr von Datendiebstahl, persönlicher Repression und Betrug</b>	<ul style="list-style-type: none"> <li>• Missbräuchliche Verwendung der Daten / Datendiebstahl</li> <li>• Grundsätzliche Bedrohung der Privatsphäre</li> <li>• Erhöhte Gefahr von persönlicher Repression (Stalking, Mobbing, Identitätsdiebstahl u.ä.)</li> <li>• Erhöhte Gefahr von Betrugs- und Täuschungsdelikten</li> </ul>	0.763	81%
<b>Big Data ermöglicht die Optimierung von Abläufen und erhöht die Agilität</b>	<p>Big Data ist ein wichtiges Mittel, ...</p> <ul style="list-style-type: none"> <li>• um Unternehmen und Organisationen ein agileres Handeln zu ermöglichen</li> <li>• um operative und logistische Abläufe optimieren zu können</li> <li>• um ein Daten- und Fakten-basiertes Handeln zu fördern</li> <li>• um genauere Prognosen und Risikoabschätzungen zu ermöglichen</li> </ul>	0.792	82%

<sup>27</sup> Cronbachs Alpha ist eine Masszahl für die interne Konsistenz einer Skala und bezeichnet das Ausmass, in dem die Fragen (Items) einer Skala miteinander in Beziehung stehen. Werte über 0.8 gelten gemeinhin als gut, Werte über 0.7 als akzeptabel und Werte über 0.6 als fragwürdig. Werte unter 0.5 gelten als inakzeptabel.

<b>Big Data ermöglicht die Personalisierung und die Identifikation von "schwarzen Schafen"</b>	<ul style="list-style-type: none"> <li>• um personalisierte Werbung zu ermöglichen</li> <li>• um intelligente, individualisierte Preismodelle zu ermöglichen</li> <li>• um die Personalisierung von Informationen und Dienstleistungen zu ermöglichen</li> <li>• um "Schwarze Schafe" unter den Wirtschaftsakteuren (z.B. schlechte Zahler) frühzeitig zu identifizieren</li> </ul>	0.827	58%
--	---	-------	-----

Tabelle 18: Auswirkungen von Big Data (Items aus Fragen B1 und B2)

Die Fragen C1, C2 und C5 beziehen sich auf **Aspekte der Data-Governance**:

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Der Staat muss intervenieren, weil der Datenmarkt nicht funktioniert.</b>	<ul style="list-style-type: none"> <li>• Der Datenschutz ist durch juristische und ökonomische Massnahmen sicherzustellen (Auflagen, Inspektionen, Bussen).</li> <li>• Der Staat muss die Geschäftspraktiken der grossen, internationalen Firmen im Internetbereich stärker regulieren und kontrollieren.</li> <li>• Der Staat muss Massnahmen ergreifen, damit der Markt im Bereich der Daten besser funktioniert.</li> <li>• Im Bereich der Daten spielt der Markt recht gut; der Staat sollte sich heraushalten [negativ codiert]</li> <li>• Natürliche Monopole (Netzwerkeffekte) führen dazu, dass der Daten-Markt in etlichen Bereichen versagt.</li> <li>• Informations-Asymmetrien führen dazu, dass der Datenmarkt in etlichen Bereichen versagt.</li> <li>• Kunden/Nutzer sind nicht in der Lage, ihre datenbezogenen Interessen gegenüber mächtigen Anbietern durchzusetzen.</li> </ul>	0.748	81%

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Der Datenschutz ist durch ein Empowerment der Nutzer sicherzustellen.</b>	<ul style="list-style-type: none"> <li>• Es sollte in der Kontrolle jeder/jedes Einzelnen liegen, welche Daten er/sie wem zu welchem Zweck preisgeben möchte.</li> <li>• Die digitale Identität gilt es gleich zu schützen wie die physische; analog zur Garantie der physischen Unversehrtheit müssen auch die Daten, die einen betreffen, korrekt sein.</li> <li>• Jede(r) Einzelne soll die Herrschaft über die ihn/sie betreffenden personenbezogenen Daten ausüben.</li> <li>• Die Datenschutzproblematik ist durch ein Empowerment der Nutzer / Kunden / Bürgerinnen zu entschärfen.</li> </ul>	0.584	91%

Tabelle 19a: Aspekte der Data-Governance (Items aus Fragen C1, C2 und C5)

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Personendaten müssen geschützt werden; ihre Preisgabe kann problematisch sein.</b>	<ul style="list-style-type: none"> <li>• Besonders zu schützen sind Daten zu Gesundheit, finanzieller Situation, Religion, politischer Zugehörigkeit u.ä.</li> <li>• Besonders zu schützen sind Daten, die es erlauben, jemanden zu identifizieren.</li> <li>• Besonders problematisch ist das Verbinden von Personendaten aus verschiedenen Quellen in einem Personenprofil.</li> <li>• Es ist aus gesellschaftlicher Sicht problematisch, wenn zu viele Menschen ihre persönlichen Daten aus individuellen Nutzenüberlegungen heraus preisgeben.</li> </ul>	0.672	86%
<b>Die Leute erhalten für die Preisgabe ihrer Daten eine faire Gegenleistung.</b>	<ul style="list-style-type: none"> <li>• Generell erhalten die Leute für die Preisgabe ihrer Daten im Internet eine faire Gegenleistung.</li> <li>• Generell erhalten die Leute für die Preisgabe ihrer Daten ausserhalb des Internets eine faire Gegenleistung.</li> </ul>	0.767	9%
<b>Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt.</b>	<ul style="list-style-type: none"> <li>• Die Einschätzung, welche Daten schützenswert sind, variiert individuell und ist auch kulturell geprägt.</li> </ul>	n/a	60%
<b>Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Personendaten ist nicht sinnvoll.</b>	<ul style="list-style-type: none"> <li>• Eine generelle Unterscheidung zwischen schützenswerten und nicht schützenswerten Daten ist nicht sinnvoll; die Frage, welche Daten schützenswert sind, muss kontextabhängig beantwortet werden.</li> </ul>	n/a	45%

Tabelle 19b: Aspekte der Data-Governance (Items aus Fragen C1, C2 und C5) (Fortsetzung)

Die Fragen B4 und B5 beziehen sich auf den **kollektiven Handlungsbedarf**:

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Förderung der Sekundärnutzung von Daten</b>	<ul style="list-style-type: none"> <li>• Förderung der Aus- und Weiterbildung von Datenspezialisten (Data Scientists, Data Journalists o.ä.)</li> <li>• Förderung der Forschung im Bereich künstliche Intelligenz</li> <li>• Förderung der Sekundärnutzung von Daten innerhalb der öffentlichen Verwaltung</li> <li>• Förderung der Sekundärnutzung von Daten in der Forschung</li> <li>• Förderung der Sekundärnutzung von Daten durch die Privatwirtschaft</li> <li>• Bereitstellung der technischen Infrastruktur für die Bereitstellung und Archivierung von sehr grossen Datenmengen</li> </ul>	0.801	62%
<b>Konsequente Umsetzung des Open-Data-Prinzips</b>	<ul style="list-style-type: none"> <li>• Konsequente Umsetzung des Open-Data-Prinzips in der öffentlichen Verwaltung</li> <li>• Konsequente Umsetzung des Open-Data-Prinzips im Bereich der Forschung</li> <li>• Konsequente Umsetzung des Open-Data-Prinzips mit Blick auf sämtliche Daten, welche im Rahmen der politischen oder behördlichen Entscheidungsfindung eine Rolle spielen (inklusive Daten aus dem privaten Sektor)</li> </ul>	0.872	70%
<b>Verschärfung der Datenschutzregeln</b>	<ul style="list-style-type: none"> <li>• Verschärfung der Datenschutzregeln für die Privatwirtschaft</li> <li>• Verschärfung der Datenschutzregeln für die Forschung</li> <li>• Verschärfung der Datenschutzregeln für Behörden</li> </ul>	0.855	53%
<b>Verstärkung von Kontrollmechanismen (Datenschützer, Wettbewerbsbehörden, Whistleblower, investigativer Journalismus)</b>	<ul style="list-style-type: none"> <li>• Verbesserung des Schutzes von Whistleblowern / Förderung des investigativen Journalismus</li> <li>• Erweiterte Kompetenzen für Datenschutzbeauftragte</li> <li>• Verstärkte wettbewerbsrechtliche Kontrolle von (Quasi-)Monopolisten im Internet-Bereich</li> </ul>	0.683	66%

Tabelle 20a: Kollektiver Handlungsbedarf (Items aus Fragen B4 und B5)

Dimension	Fragebogen-Items	Cronbachs Alpha	Anteil pos. Antworten
<b>Datenschutzlabels, rechtliche Rahmenbedingungen für Datenzentren</b>	<ul style="list-style-type: none"> <li>• Verbesserung der rechtlichen Rahmenbedingungen für sichere Datenzentren</li> <li>• Vergabe von Datenschutzlabels im Rahmen einer Zertifizierung von Unternehmen/Organisationen</li> <li>• Zertifizierung von Unternehmen und Vergabe von Datenschutzlabels zur Durchsetzung höherer Datenschutzstandards am Markt</li> </ul>	0.704	72%
<b>Standardisierung der technischen Schnittstellen</b>	<ul style="list-style-type: none"> <li>• Standardisierung von technischen Schnittstellen</li> </ul>	n/a	69%

Tabelle 20b: Kollektiver Handlungsbedarf (Items aus Fragen B4 und B5) (Fortsetzung)