Digitalisierung

Eine Datenpolitik des Vertrauens *für Fortschritt und Innovation*

12.03.2018

economiesuisse

Auf einen Blick

Die Schweiz muss die Stärken, denen sie ihren Wohlstand zu verdanken hat, auch in der digitalen Welt erhalten. Dies gilt insbesondere bei Fragen im Umgang mit Daten. Eine Mischung aus freiheitlichem Innovationsgeist und Vertrauen zwischen Wirtschaft und Gesellschaft ist erforderlich, damit die Schweiz auch in Zukunft zu den Gewinnern in einer von digitalen Entwicklungen geprägten Wirtschaft gehört. Eine Datenpolitik des Vertrauens ist der Schlüssel hierzu. Die Wirtschaft ist bereit, ihren Teil beizutragen.

Inhalt

Das Wichtigste in Kürze

Die innovative Nutzung von Daten ermöglicht ungeahntes Potenzial, eröffnet neue Anwendungsfelder und fördert die Entstehung von neuen Geschäftsmodellen. Gleichzeitig lösen die mit der digitalen Transformation verbundenen Veränderungen aber auch Verunsicherungen aus. Was geschieht mit den Daten in den Tiefen der globalen Netze? Wie kann sichergestellt werden, dass Daten nicht in falsche Hände geraten? Wie kann die Sicherheit in den vernetzten Systemen gewährleistet und kontinuierlich verbessert werden? Daraus ergeben sich Folgefragen: Wie soll die Politik auf diese Entwicklungen reagieren? Was sind dabei die Aufgaben des Einzelnen, der Wirtschaft und des Staates? Auf diese Fragen gibt economiesuisse mit ihrer Datenpolitik Antwort. Zusammen mit Vertretern aller Branchen, grosser wie auch kleiner Unternehmen, hat economiesuisse eine Datenpolitik der Wirtschaft entwickelt. Darin wird aufgezeigt, wie mit den offenen Fragen und unterschiedlichen Interessen im Spannungsfeld zur Innovations- und Wettbewerbsfähigkeit der Schweiz umgegangen werden soll – dies weit über die reinen Fragen des Datenschutzes hinaus. Die Schaffung des Vertrauens des Einzelnen in den Umgang mit den Daten ist dabei eine zentrale Aufgabe.

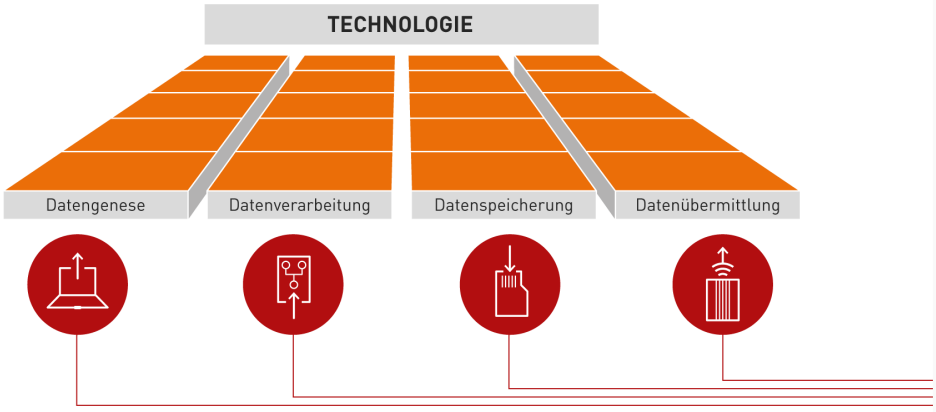
Position *economiesuisse*

- **Keine staatliche Regulierung auf Vorrat in der Datenpolitik:** Voreilige, einschneidende Regeln in einem dynamischen technologischen Umfeld bergen das Risiko, dass künftige Wertschöpfungspotenziale und Entwicklungen verhindert werden.
- **Datenschutz und Innovation nachhaltig in Einklang bringen:** Daten sind der Innovationstreiber für innovative Geschäftsmodelle. Dabei muss die Ermöglichung von Innovation in einem angemessenen Verhältnis zum Schutz der Daten des Einzelnen stehen.
- **Der Staat muss Selbstregulierung anerkennen und fördern:** Viele Herausforderungen im Datenbereich können durch Selbstregulierung besser erfasst werden, als durch eine starre staatliche Regelung. Der Staat verfügt über genügend Mittel, um Unternehmen andernfalls in die Verantwortung zu nehmen.
- **Angemessene Standards der Wirtschaft als Empfehlungen:** In vielen Bereichen kann Rechtssicherheit durch Empfehlungen der Wirtschaft, welche einen allgemeingültigen Standard für den Umgang mit Daten festlegen, geschaffen werden.
- **Die Freiheit Privater zu eigenverantwortlichem Handeln erhalten:** Staatliche Bevormundung führt beim Umgang mit Daten nicht zum Ziel. Private müssen die Möglichkeit haben, innerhalb der technologischen Rahmenbedingungen eigenverantwortlich über ihre Daten bestimmen zu können.
- **Nutzung technischer Mittel zur Vertrauenssicherung:** Neue Technologien und Konzepte müssen konsequent eingesetzt werden. Dies garantiert einen vertrauensbildenden und gleichzeitig die Eigenverantwortung fördernden Umgang mit Daten.
- **Nutzung bestehender gesetzlicher Instrumente:** Nahezu alle rechtlichen Fragen lassen sich mit dem bestehenden, etablierten Instrumentarium beantworten. Unter anderem das Bundesgesetz über den unlauteren Wettbewerb (UWG), das Urheberrechtsgesetz (URG), weitere Immaterialgüterrechte und das Kartellgesetz (KG) bieten sich hierzu an.

Die Digitalisierung ist die Grundlage, auf der Wirtschaft, Wissenschaft und Gesellschaft in Zukunft aufbauen. Die economiesuisse-Publikation «Digitale Wirtschaft» zeigt auf, was die Schweiz tun muss, um zu den Gewinnern der durch technologische Entwicklung verursachten Veränderungen zu gehören[1]. Im Zentrum der Digitalisierung steht die Möglichkeit, Daten zu generieren, diese zu verarbeiten, zu speichern und zu übermitteln[2]. Daten sind damit der eigentliche Innovationstreiber für die Gesellschaft. Alle digitalen Geschäftsmodelle bauen auf der Nutzung von Daten auf, was in den nachfolgenden Beispielen verdeutlicht werden soll.

Grafik 1

Datenprozesse im Zentrum der Digitalisierung



Quelle: eigene Darstellung
www.economiesuisse.ch

Vereinfachung der Mobilität

Bereits heute können Verkehrsmittel wie Taxis, öffentlicher Verkehr, Mietautos oder Mietvelos übergreifend in einer App erfasst werden. Diese gibt die gewünschte Route in einer Art vor, die der schnellsten und einfachsten Bewältigung dieser Route entspricht. Diese App kann auch weitere individuelle Elemente einbeziehen und so unter anderem die Lieferung von Einkäufen oder Restaurantbestellungen an den eigenen Wohnort bewerkstelligen.

(Früh-) Erkennung von Krankheiten
Zeigt ein Foto eines Kinderauges einen weissen Fleck, statt ein rotes Auge bei Blitzlichtaufnahmen, so kann das ein Hinweis auf einen Tumor im Auge liefern. Die App «White Eye Detector» durchsucht laufend auf dem Mobiltelefon gespeicherte Fotos nach Warnsignalen für Augenkrebs. Auffällige Augen werden von der App sofort erkannt und gemeldet. Ferner kann die App mithilfe der Handykamera einen Augenkrebs-Schnelltest durchführen. Auch mittels Google-Algorithmen können anhand von Bildern der Augen Krankheiten festgestellt werden. So wurde beispielsweise kürzlich eine Anwendung entwickelt, mit der es möglich ist, erhöhten Blutdruck und das Risiko eines Herzinfarkts zu ermitteln. Im Vergleich zu konventionellen Methoden ist dies eine kostengünstigere, schnellere und nicht invasive Variante.

Patienten im Medizinbereich besser unterstützen und neue Therapien entwickeln
Medizinische Hilfsmittel zur Behandlung einer Krankheit (wie beispielsweise ein Inhalationsgerät) können bald mittels Sensoren und einer App dem behandelnden Arzt Daten und Messwerte liefern. Dies ermöglicht dem Arzt eine bessere Auswertung. Arzt und Patient erhalten unmittelbar Informationen über den Therapieverlauf, Nebeneffekte oder Infektionen. Falls nötig könnte dies einen sofortigen Eingriff erlauben. Auf diese Weise grossflächig erfasste Daten ermöglichen neue Erkenntnisse zur Verbesserung der Therapien für andere Patienten.

Planeten und Galaxien entdecken
2017 entdeckte die Nasa (National Aeronautics and Space Administration) mit Hilfe von Google ein neues Sonnensystem mit acht Planeten, das unserem Sonnensystem ähnelt. Der Suchmaschinenkonzern wertete dazu Daten des Kepler-Teleskops aus. Es war dabei möglich, innerhalb kürzester Zeit wesentlich mehr Daten auszuwerten als von Hand: Das Kepler-Teleskop hat innerhalb von vier Jahren 200'000 Sterne beobachtet und alle 30 Minuten ein Foto gemacht. Damit wurden Billionen von Daten gesammelt. Astronomen hätten für diese Auswertungen ein Vielfaches an Zeit gebraucht.

Daten über Daten

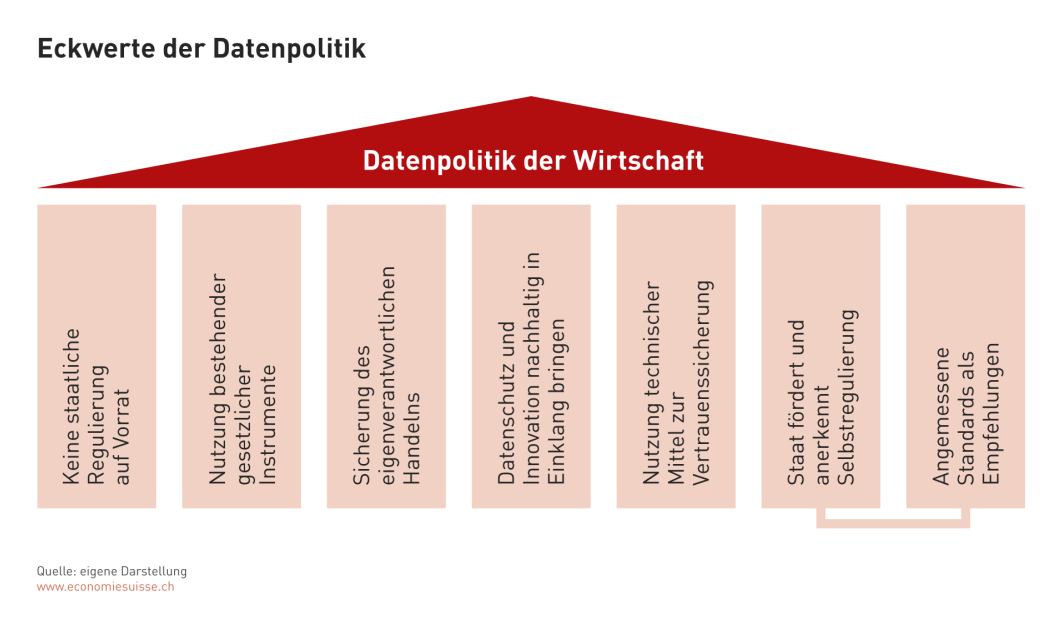
Im Jahr 2016 wurden weltweit 16,1 Zettabytes Daten produziert. Ein mit Schreibmaschine geschriebener Text desselben Datenvolumens hätte einen Umfang von 230 Billiarden A4-Seiten. Das entspricht einem Stapel mit der Höhe der 82-fachen Distanz zwischen Sonne und Neptun. Das Licht bräuchte 14 Tage und acht Stunden, um vom Ende des Stapels zur Erde zu gelangen (Vgl. economiesuisse/W.I.R.E., Zukunft digitale Schweiz, a.a.O., S. 15.).

Eine der Herausforderungen von Unternehmen ist es, das Vertrauen des Einzelnen bei der Verwendung von Daten zu sichern. Ohne Vertrauen ist keine nachhaltige Datenwirtschaft möglich. Der Einzelne bietet seine Daten dann an, wenn er weiss, dass ein angemessener Umgang damit gewährleistet ist. Transparenz bei der Datenerfassung und -verwendung ermöglicht es dem Einzelnen, dabei entscheiden zu können, welche Angebote er nutzen will und welche nicht.

Grundlegende Pfeiler der Datenpolitik

Mit ihren Eckwerten definiert die Wirtschaft die grundlegenden Pfeiler einer Datenpolitik. Daraus leiten sich Forderungen und Handlungsfelder her, auf die in diesem Dossier vertieft eingegangen wird. Im Sinne eines konstruktiven Beitrags wird so aufgezeigt, wie mit Daten innerhalb der Spannungsfelder von unterschiedlichen Interessen umzugehen ist.

Grafik 2



Wir und unser Umfeld erzeugen konstant Daten. Sei dies durch unsere Aktivitäten im Internet, durch die Nutzung von Produkten, dem Tätigen von Finanztransaktionen, dem Besuch eines Fitnesscenters oder dem Ausfüllen der Steuererklärung. Auch Maschinen erzeugen Daten, denn sie erfassen beispielsweise Betriebszustände oder kommunizieren Produktionsdaten. Daten entstehen überall und jederzeit.

Forderungen und Handlungsfelder

Aus den aufgezeigten übergeordneten Eckwerten der Datenpolitik ergeben sich die folgenden Forderungen und Handlungsfelder:

1. Keine Schaffung von Dateneigentum.
2. Der Datenverkehr darf nicht neuartig gesetzlich eingeschränkt werden.
3. Bestehende gesetzliche Instrumente gewährleisten den Zugang zu Daten und sichern Investitionen in datenbasierte Produkte.
4. Vertrauen als Grundlage für Datenbearbeitung und Innovation.
5. Kein grundsätzlicher gesetzlicher Anspruch auf Datenportabilität.

6. Anonymisierungsstandards der Wirtschaft.
7. Förderung des risikobasierten Ansatzes bei der Daten-Governance.
8. Unterstützung von Open Government Data (OGD).
9. Branchenspezifische Mindestanforderungen für Cybersecurity und Verbesserung des Bedrohungs- und Krisenmanagements.

Best Practices sind der staatlichen Regulierung auf Vorrat klar überlegen

In den Gebieten, in denen es nötig ist, Klarheit zu schaffen, braucht es in den wenigsten Fällen Interventionen des Gesetzgebers. Die Gesetzgebung kann einerseits mit den dynamischen Entwicklungen gar nicht mithalten. Andererseits geht es bei den grundsätzlichen Fragen des Vertrauens um einen Austausch zwischen Wirtschaft und Gesellschaft. Best Practices der Wirtschaft können dieses Vertrauen besser und effizienter entwickeln, als dies gesetzliche Regulierung auf Vorrat täte.

1. Keine Schaffung von Dateneigentum

Der Begriff des Dateneigentums ist derzeit in aller Munde. Dieses wird als Lösung angepriesen, wie Private die Hoheit über ihre Daten erhalten und Unternehmen ihre Investitionen schützen sollen. Die Forderung wird auch schon in der Politik geltend gemacht. Doch ist ein Eigentumsrecht an Daten gerechtfertigt und wie könnte es umgesetzt werden?

Die Ausgangslage bei sachenrechtlichen Denkmustern hat sich im Rahmen der technologischen Entwicklung dynamisiert. Bislang nur theoretisch denkbare oder nur schwer umsetzbare Formen der Ausübung von Besitz und Eigentum sind heute möglich: Die Verfügbarkeit von Informationen verhindert Suchkosten und führt Leute mit gleichgerichteten Bedürfnissen zusammen. Dies sieht man bei den neuen Formen von Verleih (so z. B. Uber und Airbnb) oder darin, dass wir heute Inhalte häufig nicht mehr besitzen, sondern nutzen (so z. B. Streaming-Dienste). So kann ein Film auf einer DVD nur von einem Nutzer angesehen werden, der die DVD physisch besitzt; ein Film auf Netflix ist zur gleichen Zeit einer Vielzahl von Personen zugänglich.

Zurzeit sind Daten nicht als Rechtsobjekte definiert. Es können damit auch keine absoluten Rechte wie beispielsweise Eigentumsrechte daran geltend gemacht werden. Dennoch stellt das geltende Recht für alle Beteiligten einen geeigneten Umgang mit den Daten sicher. Die Einführung eines solchen Rechtsobjekts und damit auch eines Dateneigentums ist entsprechend nicht notwendig. Insbesondere steht die Schaffung eines Dateneigentums quer zu

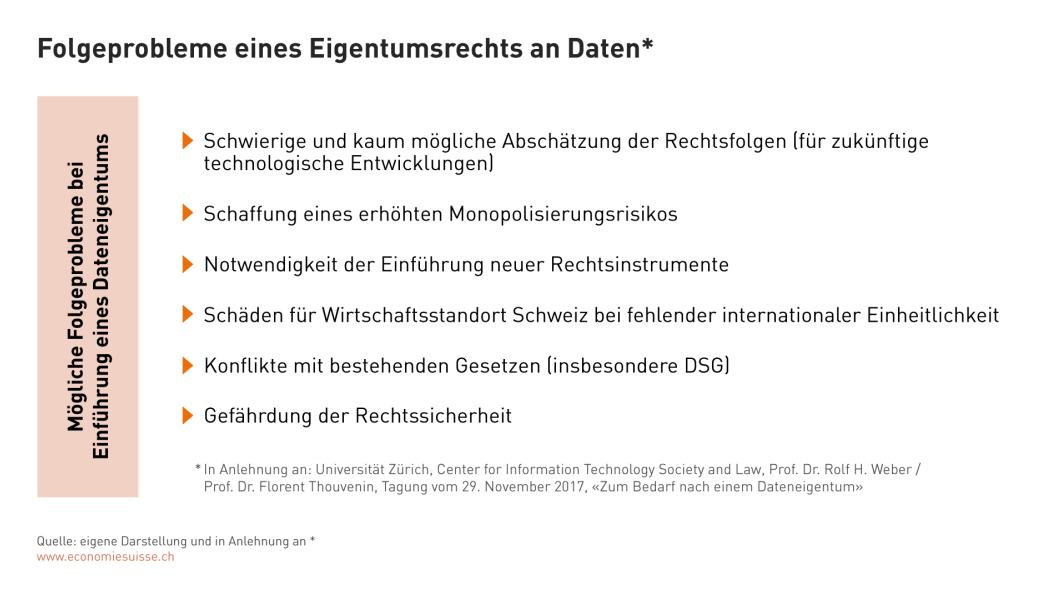
den Ansprüchen und Errungenschaften der Digitalisierung. Sollten spezifische Bereiche einer rechtlichen Anpassung bedürfen – beispielsweise im Kontext von Blockchain[3] –, so können solche Anpassungen der Rechtsordnung punktuell und gezielt vorgenommen werden, ohne dass dadurch eine ungewollte Gesamtwirkung auf die digitalisierte Wirtschaft entsteht.

Eine weitere Problematik ist, dass die Ansprüche an die Ausgestaltung von solchen Rechten nicht fassbar sind. Bei einer rechtlichen Fixierung von Daten wäre bei einer fehlenden internationalen Abstimmung auch die Rechts- und Planungssicherheit massiv gefährdet. Es gibt andere hinreichende Methoden, um den Datenschutz zu gewährleisten und Investitionen zu bewahren. So ermöglicht beispielsweise das Persönlichkeitsrecht den Schutz des Individuums auch im Bereich der Datenwirtschaft.

Das Gesagte gilt auch für Algorithmen
Algorithmen sind Handlungsanweisungen für Maschinen, so wie Kochrezepte eine Anleitung zum Kochen sind. Eine neuartige gesetzliche Einschränkung von Algorithmen wäre ebenso wie bei einem Eigentumsrecht an Daten verfehlt und würde die Entwicklung in diesem Bereich hemmen. Denn Algorithmen schaffen schliesslich einen wesentlichen Mehrwert aus Daten:

- Die Google-Suchmaschine beantwortet Suchanfragen auf Basis von Algorithmen;
- Navigations-Apps weisen mithilfe von Algorithmen den Weg;
- Algorithmen in der Bankenbranche ermöglichen die Risikobeurteilung bei Kreditgeschäften.

Grafik 3



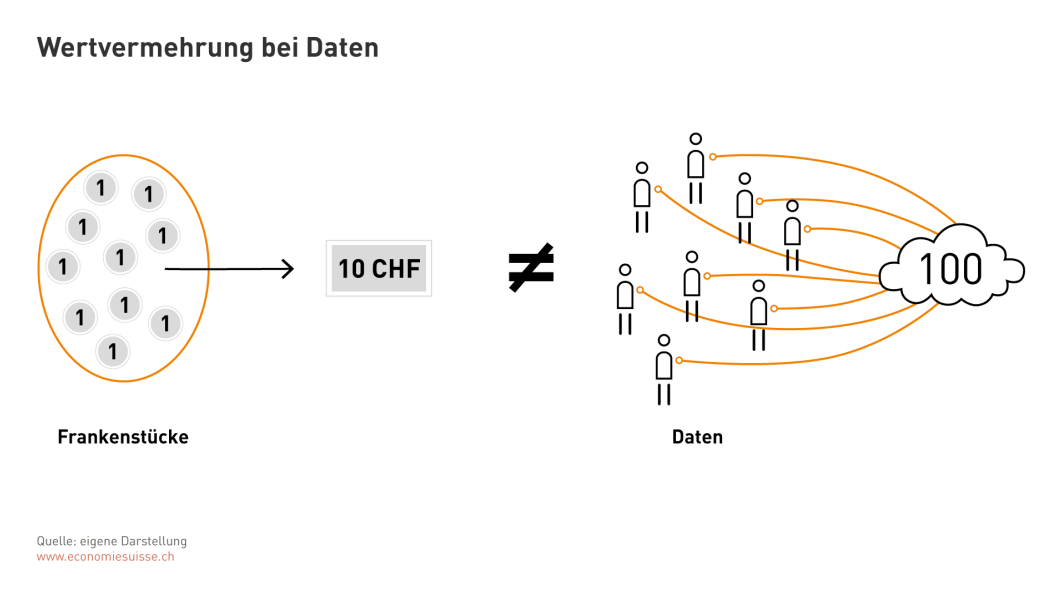
Ein Klärungsbedürfnis bei neuartigen Geschäftsmodellen kann ausnahmsweise bestehen, so beispielsweise bei Daten im Konkurs. Durch die Auslagerung von Fotos auf eine Cloud kann der Speicherplatz des Mobiltelefons über das Gerät hinaus vergrössert werden. Auch Unternehmen benutzen den Speicher in der Cloud wegen des vereinfachten Zugriffs und aufgrund weiterer Dienstleistungen von Cloud-Anbietern. Fällt nun ein Anbieter von Cloud-Lösungen in Konkurs, so besteht für ein Unternehmen keine Möglichkeit, die Herausgabe der Daten im Cloud-Speicher zu verlangen. Dies obwohl die betreffenden Daten für den Geschäftsbetrieb notwendig sind. Das liegt daran, dass Daten rechtlich gesehen keine konkursrelevanten beweglichen Sachen darstellen. In solchen Fällen kann eine Regelung der Rechte an Daten ausnahmsweise sinnvoll sein.[4]

Der Wert von Daten ergibt sich erst, wenn sie in einem spezifischen Kontext stehen

Besitzt man ein Frankenstück, so kann man sich damit Ware im entsprechenden Gegenwert kaufen. Wenn zehn Leute je einen Franken zusammenlegen, so ergibt das zehn Franken. Bei Daten bemisst sich der Wert auf eine andere Art. Ein einzelnes Datum hat für sich keinen Wert. Erst wenn Daten in einen Kontext bezüglich Herkunft oder anderen Datensätzen

gestellt werden, kann ein Wert entstehen. So können einzelne unbedeutende Bewegungsdaten in ihrer Kombination für ein Veloverleihsystem plötzlich von Bedeutung werden, da sie dann Informationen liefern, die vom Unternehmen interpretiert werden können. Dieser Wert lässt sich nicht auf das einzelne Datum zurückrechnen.

Grafik 4



2. Der Datenverkehr darf nicht neuartig gesetzlich eingeschränkt werden

Als Datenverkehr versteht man den Fluss von Daten innerhalb von digitalen Übertragungswegen zwischen unterschiedlichen Beteiligten. Immer wenn Informationen weitergegeben werden, findet in einem weiten Sinn auch Datenverkehr statt. Für die Beteiligten am Datenverkehr bestehen Rechte und Pflichten. Die Uneingeschränktheit des Datenverkehrs, unabhängig vom Standort der Beteiligten (d. h. auch international), ist von grundlegender Bedeutung für die Wirtschaft. Jegliche staatlich angeordnete Einschränkungen oder neuartige gesetzliche Regulierungen sind abzulehnen. Dies gilt insbesondere auch für Netzsperren.

Netzsperren sind abzulehnen

Bei Netzsperren oder Zugangsbeschränkungen handelt es sich um technische Massnahmen, mit denen die Erreichbarkeit von bestimmten Dienstleistern im Internet auf staatliche Anordnung eingeschränkt wird. Beispielsweise sieht der Gesetzesentwurf zum Geldspielgesetz Netzsperren vor. Damit sollen nicht konzessionierte ausländische Anbieter vom Schweizer Geldspielmarkt ausgeschlossen werden. Die Internetnutzer sollen durch staatlich kontrollierte und von den Internetprovidern durchzusetzende technische Barrieren daran gehindert werden, die Webseiten mit den entsprechenden Angeboten aufzurufen. Solche Sperren sind hierfür nicht nur völlig ungeeignet, sie sind darüber hinaus gefährlich, da sie die Sicherheit und Stabilität im Internet beeinträchtigen.

Datenverkehr: Privatautonomie und Best Practices bringen Vorteile

Beteiligte, Private und Unternehmen, regeln den Verkehr von Daten bereits heute unter sich. Dies erfolgt in der Regel gestützt auf vertragliche Vereinbarungen, Nutzungsbedingungen und unter Verwendung der bestehenden gesetzlichen Bestimmungen. Eine zusätzliche gesetzliche Regelung ist dabei nicht notwendig.

Best Practices sind Verhaltensstandards, welche sich Branchen oder die Wirtschaft selbst auferlegen. Im Bereich Datenverkehr können mithilfe von Best Practices eine ungenügende Information des schwächeren Beteiligten vermieden und die Sicherheit des Datenverkehrs gefördert werden. Dadurch lässt sich ein verantwortungsvoller Umgang mit den Daten gewährleisten. Best Practices sind unter anderem in folgenden Formen möglich:

- Standardklauseln/Vertragselemente mit fair ausgewogenen Rechten und Pflichten der Beteiligten, welche von diesen im Rahmen von Verträgen übernommen werden können;
- Technische Standards bezüglich Technologie und Sicherheit;
- Einheitliche Rollenbezeichnung der Beteiligten beim Datenverkehr.

Best Practices gewährleisten nicht nur die Verantwortung der Beteiligten im Datenverkehr, sondern führen auch, beispielsweise durch standardisierte

Vertragselemente, zu dessen Beschleunigung und Vereinfachung. Schliesslich schaffen sie Rechtssicherheit.

Medienbrüche verlangsamen Geschäftsprozesse
Von einem Medienbruch spricht man, wenn bei einer digitalisierten Informationsübermittlung oder -verarbeitung Informationen manuell übertragen (beispielsweise per Hand in einen Computer eingegeben) werden müssen. Solche Medienbrüche können gerade im Austausch mit Behörden zu einem grossen Mehraufwand führen. Wenn eine Information, die im Unternehmen elektronisch verarbeitet wurde, zwecks Einreichen bei einer Aufsichtsbehörde manuell aufbereitet (beispielsweise auf Papier gebracht oder in eine Online-Maske eingetippt) werden muss, bedeutet das zusätzlichen Zeitaufwand, zusätzliche Fehlerquellen und somit eine Qualitätseinbusse für den entsprechenden Prozess. Gerade im Verhältnis zum Staat lähmen solche Medienbrüche regelmässig einen effizienten Austausch. Das Seco hat im Sommer 2017 in der Wirtschaft eine Umfrage zur digitalen Tauglichkeit von Gesetzen durchgeführt (digitaler Test): Dabei wurden zahlreiche Bestimmungen identifiziert, die einem digitalen Austausch mit den Behörden im Weg stehen.

3. Bestehende gesetzliche Instrumente gewährleisten den Zugang zu Daten und sichern Investitionen in datenbasierte Produkte

Daten, die eine Person allgemein preisgibt, entziehen sich zu einem bestimmten Grad ihrer Kontrolle. Solche Daten können sich bei einer öffentlichen Verwaltung, einem Unternehmen oder einer anderen Person befinden. Zugangsrechte setzen sich damit auseinander, wer welche Berechtigungen an Daten hat. Dies gilt beispielsweise auch im Verhältnis zwischen zwei Unternehmen.

Beim Investitionsschutz geht es darum, die mit Daten verbundenen Aufwendungen angemessen vor unzulässiger Verwertung durch Dritte zu schützen. Eine Entwicklung im Bereich datenbasierter Produkte soll nicht (oder zumindest nicht ohne eine Entschädigung) von einem Dritten verwendet werden dürfen.

Beispiele: Gesetze wie UWG, KG und URG bieten zahlreiche Möglichkeiten

- Richtig eingesetzt, verfügen wir über ein funktionierendes gesetzliches Instrumentarium, um eine faire Regelung des Zugangs zu Daten und den Schutz von Investitionen in datenbasierte Produkte zu gewährleisten:
- Das Bundesgesetz über den unlauteren Wettbewerb (UWG) sieht ein sogenanntes Leistungsschutzrecht vor. Das heisst, dass die Verwendung einer eigenen Leistung durch einen Dritten gerichtlich verhindert werden kann.
- Die Thematik, dass Unternehmen Zugang zu Daten von anderen Unternehmen fordern, um auf einem bestimmten Markt tätig zu sein, ist nicht neu. So wurde diese Thematik schon immer aus kartellrechtlicher Perspektive (KG) im Rahmen der Missbrauchskontrolle abgehandelt. Das Schlagwort Essential Facility dürfte hierbei zeitnah in Verbindung mit Daten auftauchen.
- In der Europäischen Union (EU) ist ein spezifischer Schutz für Datenbanken der eigenen Art gesetzlich vorgesehen. Eine solche Regelung ist jedoch entbehrlich. So können Datenbanken im Schweizer Recht unter gewissen Voraussetzungen in den Schutz des Urheberrechts (URG) gelangen. Ein hinreichender Schutz wird auch hier insbesondere durch das Leistungsschutzrecht des UWG gewährleistet.

Streitigkeiten können durch Gerichte gestützt auf bestehende gesetzliche Instrumente sachgerecht beurteilt werden

Das Bundesgericht beschäftigte sich 2005 mit einer Streitigkeit zwischen mehreren Anbietern von Online-Immobilien-Inseraten. Dabei durchforstete ein Unternehmen das Internet systematisch nach veröffentlichten Immobilien-Inseraten und schaltete diese auf der eigenen Website auf. Dies tat es, um die Inserate auf diese Weise kommerziell zu verwerten. Das Bundesgericht beschäftigte sich mit der Frage, ob dies zulässig ist. Nach einer umfassenden rechtlichen Abwägung löste das Bundesgericht den Fall abschliessend gestützt auf das Bundesgesetz über den unlauteren Wettbewerb (UWG).

4. Vertrauen als Grundlage für Datenbearbeitung und Innovation

Der Nutzer will heute vermehrt die auf ihn passenden und für ihn interessanten Inhalte jederzeit überall und auf Abruf verfügbar haben. Die Loyalität zu einem Anbieter steht oft nicht mehr im Vordergrund, sondern die Informations-, Waren- und Dienstleistungsbeschaffung. Neue Geschäftsmodelle gehen auf die Bedürfnisse solcher Nutzer ein. So entstehen durch die Digitalisierung Chancen für neue Dienstleistungen, zusätzlichen Komfort und eine grössere Angebotsvielfalt. Die Arbeit mit grossen Datenmengen steht dabei im Zentrum von zahlreichen neuen Geschäftsmodellen. Derjenige, der Daten zur Verfügung stellt, muss darauf vertrauen können, dass sachgerecht mit diesen Daten umgegangen wird. Es muss sichergestellt sein, dass seine Daten nicht für sachfremde Zwecke missbraucht werden. Was für den einen Nutzer akzeptabel ist, mag für den anderen zu weit gehen. Der Wunsch des Individuums muss bei der Frage, was zulässig ist und was nicht, im Zentrum stehen. Ein übertriebener, bevormundender Datenschutz führt daher gerade in diesem Bereich zu einer massiven Einschränkung neuer Entwicklungen. Das Spannungsverhältnis zwischen Datenschutz einerseits und Innovationsfähigkeit andererseits muss dabei zwischen Nutzern und Anbietern in Einklang gebracht werden.

Ethische Überlegungen, Selbstregulierung und Best Practices der Wirtschaft bei der Datenbearbeitung

Die Möglichkeiten, welche die Analysen von grossen Datenmengen bieten, sind gross. China beispielsweise versucht, über sogenanntes Big Nudging die ganze Bevölkerung im Sinne der Regierung zu bestimmten Verhaltensweisen zu bewegen. Solche Formen von Manipulation und Kontrolle sind klar abzulehnen. Bezeichnenderweise ist es oft der Staat, der aus unterschiedlichen Gründen auf Daten der Bürger zugreift. Stichworte sind dabei die Snowden-Affäre oder die Speicherung von Daten auf Vorrat für spätere Auswertungen.

Für die Wirtschaft ist es dabei von grundlegender Bedeutung, mittels ethischer Grundsätze die Grenzen von dem, was aus Sicht der

Wirtschaft gemacht werden darf, aufzuzeigen. So muss beispielsweise die Gefahr verhindert werden, dass Kunden manipuliert werden oder intransparente Prozesse zu unvorteilhaften Entscheiden führen. Die Wirtschaft ist bereit, sich im Bereich der Datenbearbeitung gestützt auf ethische Überlegungen selbst zu regulieren. Dies, da sie sich dem Vertrauen ihrer Kunden würdig zeigen will.

Aktuelle Revision der Datenschutz-Gesetzgebung und Verhältnis zur Digitalisierung

Die Wirtschaft anerkennt die Bedeutung eines angemessenen Datenschutzes. In Europa wurden die Regeln unlängst verschärft, mit direkten Auswirkungen auf die Schweiz[5]. Das Schweizer Datenschutzgesetz (DSG) befindet sich entsprechend aktuell in Revision.

Der Datenschutz bezieht sich auf den Erstgebrauch von Daten (Sammeln, Speichern und Definieren von Daten). Die digitale Transformation kann längerfristig jedoch nicht hinreichend mittels dieses überholten Ansatzes von Datenschutz erfasst werden.

5. Kein grundsätzlicher gesetzlicher Anspruch auf Datenportabilität

Datenportabilität beschäftigt sich mit der Übertragbarkeit von Daten auf andere Systeme. So gibt man beispielsweise mittels eines Facebook-Profils durch seine Aktivitäten über die Jahre hinweg unterschiedliche Daten in die Plattform ein: Freundschaften, Likes, Upload von Fotos usw. Dadurch kann der Anbieter der Plattform weitere (Daten-)Aussagen aus dem entsprechenden Verhalten herleiten. Entscheidet man sich nun für eine andere Social-Media-Plattform, stellt sich im Rahmen der Datenportabilität die Frage, ob man die eingegebenen Daten und die dadurch gewonnenen Aussagen zurückhaben und zum neuen Social-Media-Anbieter mitnehmen kann. Bei der Datenportabilität geht es also darum, ob Firmen verpflichtet werden sollen, über Nutzer erfasste Daten in strukturierter Form zu übergeben, beziehungsweise an bezeichnete Dritte weiterzugeben.

Absolute Datenportabilität schiesst über das Ziel hinaus
Firmen und Behörden sind gemäss der neuen Gesetzgebung der EU zur Datenportabilität verpflichtet. Diese Pflicht soll eine bessere Kontrolle seitens der Nutzer sicherstellen und den Wettbewerb zwischen den Dienstleistungsanbietern fördern. Verbraucher hätten dann beispielsweise einen Anspruch auf Rohdaten oder Daten von intelligenten Stromzählern, Suchmaschinen und Fitness-Wearables. Das Schweizer Recht kennt keinen solchen absoluten Anspruch auf Datenportabilität.

Am eingangs genannten Beispiel erkennt man die Einschränkungen eines absoluten Konzepts. Dem Nutzer eines sozialen Netzwerks bringt es in der Regel nichts, wenn er seine Daten ausgehändigt bekommt. Für den Nutzer sind primär die mit seinen Daten hergestellten Erkenntnisse und Aussagen interessant, gerade auch in Bezug auf Dritte. Deren Daten aber lassen sich nicht aus dem System herausholen, ohne dass man in Konflikt mit deren Interessen gerät.

Alternativen zur absoluten Datenportabilität
Unternehmen tätigen im Bereich des Ausbaus des Datenschutzes regelmässig erhebliche finanzielle Investitionen. Eine Herausgabe von Daten, die von beiden Parteien, Kunde und Unternehmen verabredet wurde, ist jederzeit möglich. Es wäre aber verfehlt, das Unternehmen auf jeden Fall zu zwingen, Daten herauszugeben und ihm dabei noch technische Vorschriften über die Art und Weise der Herausgabe zu machen. Erschweren würde eine Herausgabe zusätzlich, dass solche Daten oftmals bereits anonymisiert im System gespeichert sind oder sich gar nicht mehr einem Einzelnen zuordnen lassen. Ferner kann eine nahtlose Übertragung von einem Anbieter auf einen Privaten je nach gesetzlichen Formatvorgaben mit technischen Schwierigkeiten behaftet sein.

Für vernünftige, sachgerechte Ansprüche auf Datenherausgabe bestehen andere Möglichkeiten:

- Nutzung bestehender technischer und rechtlicher Instrumente;
- Abreden zwischen den Parteien, eventuell mittels Verträgen;
- Best Practices.

6. Anonymisierungsstandards der Wirtschaft

Anonymisierung und Pseudonymisierung stellen Massnahmen des Datenschutzes dar. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (Buchstaben- oder Zahlenkombination) ersetzt. Durch die Anonymisierung werden Daten so verändert, dass diese nicht mehr einer Person zugeordnet werden können.

Will der Professor einer Hochschule beispielsweise seinen Studenten die Ergebnisse einer schriftlichen Prüfung einfach zugänglich machen, so kann er die Studenten bitten, während der Prüfung ein selbst gewähltes Pseudonym auf den Blättern zu notieren. Nach der Korrektur kann der Professor einen Aushang (auch im Internet) veröffentlichen, wonach alle ihre Ergebnisse aus dem Schema Pseudonym/Note herauslesen können. Die Zuordnung des Pseudonyms zum jeweiligen Studenten kann nur durch den Professor oder durch den jeweiligen einzelnen Studenten hergestellt werden. Um eine Anonymisierung würde es sich handeln, wenn im Nachhinein die Prüfungsblätter mit den von den Studenten notierten Pseudonymen zerstört würden. Die Angaben auf dem Notenaushang wären für die Allgemeinheit anonymisiert, da keine Zuordnung zu den jeweiligen Studenten mehr möglich wäre.

Vorteile von Anonymisierungsstandards der Wirtschaft
Unternehmen können bei der Erarbeitung neuer Konzepte nicht zweckmässig mit Daten arbeiten, wenn sie jedes Mal eine Einwilligung beim Datengeber einholen müssen. Auch interessiert sie der personenbezogene Teil der Daten in der Regel bei solchen Arbeiten nicht. Anonymisierung und Pseudonymisierung ermöglichen und vereinfachen damit den Umgang mit solchen Daten unter Aufrechterhaltung des Persönlichkeitsschutzes.

Anonymisierungskonzepte, die auch die Möglichkeiten von Pseudonymisierung enthalten, veralten schnell. Statt starrer Vorgaben braucht es an dieser Stelle zuverlässige Standards der Wirtschaft, die sich stetig weiterentwickeln und so den Schutz der Persönlichkeitsrechte sichern.

Anonymisierungen wirken zusätzlich dem Umstand entgegen, dass die Abgrenzung zwischen Personen- und Sachdaten in der Praxis kaum möglich ist. Viele Daten, so auch beispielsweise die Betriebsdaten einer Fräsmaschine,

können einen personenbezogenen Bezug haben, wenn sie zum Beispiel mit einem Zeitstempel versehen sind und mit dem Einsatzplan der Mitarbeitenden verknüpft werden. Dadurch sind Aussagen über das Bedienerverhalten des Maschinennutzers möglich. Will man nun die Betriebsdaten zur Verbesserung von Fertigungsprozessen nutzen, können die Persönlichkeitsrechte des Maschinennutzers in die Quere kommen. Eine Anonymisierung ermöglicht die weitere Bearbeitung und Analyse der Daten bei optimalem Schutz der Persönlichkeitsrechte.

7. Förderung des risikobasierten Ansatzes bei der Daten-Governance

Die Daten-Governance eines Unternehmens beschreibt das gesamte Management der Verfügbarkeit, Verwendbarkeit, Integrität und Sicherheit von Daten, die in diesem Unternehmen verwendet werden. Die Implementierung eines Daten-Governance-Systems in einem Unternehmen beinhaltet diverse Schritte. Angefangen wird bei der Definition des Datenbestands, über die Regelung der internen Zuständigkeiten für bestimmte Datensätze bis zur Etablierung eines Kontrollmechanismus und Schulungen der Mitarbeitenden.

Beim risikobasierten Ansatz werden die grössten Investitionen in den Schutz von Daten dort vorgenommen, wo das grösste Risikopotenzial besteht. Erhebt ein Unternehmen Daten, beispielsweise mittels einer personalisierten Kundenkarte, mit der man beim Einkauf Treuepunkte sammeln kann, so entstehen für die dadurch gesammelten Daten an sich noch keine besonderen Risiken. Mittels Big-Data-Analysen[6] eröffnen sich jedoch viele Möglichkeiten für die Datenbearbeitung. So kann die Kombination der Treuepunkte mit Daten der Krankenkasse der gleichen Person durchaus bedeutend sein. Unternehmen werden in diesem risikoreicheren Bereich mehr Mittel für den Datenschutz und für die Gewährleistung von ethischen Standards aufwenden als bei anders gelagerten Daten.

Nur der risikobasierte Ansatz kann Risiken adäquat erfassen

Der risikobasierte Ansatz bei der Daten-Governance ist notwendig, um der Komplexität eines Unternehmens und den unterschiedlichen Kombinations- und Verwendungsmöglichkeiten von Daten gerecht zu werden. Daten können aufgrund ihrer Kombinationsmöglichkeiten zu verschieden stark ausgeprägten

Risikosituationen führen. Ferner gibt es in einem Unternehmen noch weitere Faktoren, die beachtet werden müssen: Es bestehen unstrukturierte Daten; Drittparteien, die auf Daten zugreifen können; Prozesse, in denen wichtige Personendaten verarbeitet werden, oder Daten, die nur auf Applikationsebene bestehen. Durch den risikobasierten Ansatz kann den grössten Risikosituationen die grösste Aufmerksamkeit gewidmet werden. Dabei werden die Ressourcen eines Unternehmens gezielt bei den tatsächlichen Risiken eingesetzt und es riskiert nicht, sich zu verzetteln.

8. Unterstützung von Open Government Data (OGD)

Die Datenbestände des öffentlichen Sektors sind vielfältig und von grossem Umfang. So sammeln Verwaltungen regelmässig unterschiedliche Daten im Rahmen ihrer amtlichen Aufgaben. Dazu gehören unter anderem Bevölkerungsstatistiken, Wetterdaten, topografische Aufzeichnung der Gemeindegrenzen der Schweiz, historische Dokumente, Verkehrsdaten oder Verzeichnisse der Schweizer Literatur. Diese Daten können nicht nur der Verwaltung, sondern auch Dritten, beispielsweise einem Unternehmen oder privaten Personen als Mehrwert dienen. Das Unternehmen hat gegebenenfalls ein Interesse, solche Daten weiterzuverarbeiten oder neu zu nutzen. So ist es möglich, dass die verfügbaren Daten neu kombiniert werden und dadurch nicht nur ein Geschäftsmodell ermöglichen, sondern ein Mehrwert für die ganze Bevölkerung schaffen.

OGD müssen der Öffentlichkeit zur Verfügung stehen

Alle diese Daten, die der Staat in der Ausführung einer hoheitlichen Aufgabe erhebt und die nicht personenbezogen sind (d. h. keine Rückschlüsse auf ein Individuum zulassen), müssen der Allgemeinheit und damit auch der Wirtschaft offenstehen. Es gilt jedoch Grenzen zu ziehen: Private, die mit dem Staat zusammenarbeiten, oder staatliche Unternehmen, die privatwirtschaftlich auftreten, sind von der Verpflichtung, die Daten herauszugeben, befreit. Auf der anderen Seite müssen staatliche Betriebe den Regeln des Wettbewerbs unterstellt werden, wenn sie privatwirtschaftlich auftreten.

Was ist «OGD»?

Bei Open Government Data (OGD) handelt es sich um Daten, die im Rahmen der hoheitlichen Tätigkeit des Staates durch diesen erhoben wurden. Die Erhebung solcher Daten wurde damit durch Steuern und Abgaben finanziert.

9. Branchenspezifische Mindestanforderungen in der Cybersecurity und Verbesserung des Bedrohungs- und Krisenmanagements

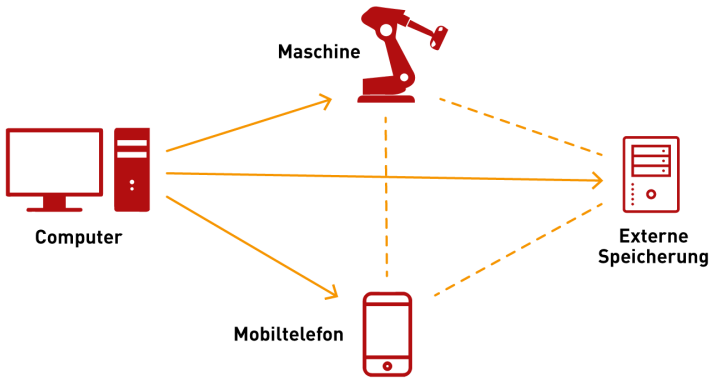
Die Digitalisierung und die damit verbundene Vernetzung von Systemen führt dazu, dass wir auf einer ganz neuen Ebene verwundbar werden. Durch den Einsatz der Technologien und deren Vernetzung, Komplexität und Dynamik entstehen Gefahren. Dies wird fast täglich durch Medienberichte über Angriffe und Manipulationen vermittelt. Diese kriminellen Aktivitäten erfolgen aus unterschiedlichsten Motivationen und mit verschiedensten Vorgehensweisen. Gleich wie wir es in der physischen Welt machen, müssen wir uns auch in der digitalen Welt vor kriminellen Taten Dritter schützen.

Branchenspezifische Minimalstandards der Wirtschaft

Ein einheitlicher, staatlich vorgeschriebener Sicherheitsstandard kann den Herausforderungen der Cyber-Kriminalität nicht gerecht werden, da dadurch das Risiko einer einseitigen und dadurch ungenügenden Cyber-Sicherheit entsteht. Vielmehr braucht es ein flexibles und dezentrales System. Wo branchenspezifisch angezeigt, kann die Wirtschaft mittels vorformulierten Minimalstandards die Cyber-Sicherheit erhöhen. Den schwächeren Gliedern in der Kette muss dabei besondere Aufmerksamkeit gewidmet werden, da ein unterdurchschnittliches Schutzniveau durch die Vernetzung mit anderen Systemen auf andere Unternehmen übertragen wird. Dies macht durch die Wirtschaft formulierte Minimalstandards in diesem Bereich umso wichtiger, da schlechter geschützte Unternehmen so vom Know-how anderer Unternehmen profitieren können. Dadurch werden auch Asymmetrien im Cyber-Bereich zwischen den Branchen vermieden. Ferner kann durch die Schaffung von Minimalstandards der risikobasierte Ansatz zur Anwendung gelangen: Die Umsetzung erfolgt in einem für das Unternehmen angemessenen Verhältnis zum Risiko. Die Vernetzung findet insbesondere auch zwischen Geräten statt. Wenn solche innerhalb eines Unternehmens nicht regelmässig gewartet werden, können sie als Startpunkt für eine Attacke verwendet werden.

Grafik 5

Übertragung von Cyber-Risiken aufgrund der Vernetzung von Gegenständen und Unternehmen



Quelle: eigene Darstellung
www.economiesuisse.ch

Es braucht eine Zuordnung der Aufgaben zwischen Privatwirtschaft und Staat für den Krisenfall und eine Förderung der Meldung von Cyber-Attacken
Im Verhältnis zwischen der Privatwirtschaft und dem Staat ist eine klare Zuordnung der Aufgaben für den Krisenfall notwendig. Der Staat soll mit den nötigen Mitteln ausgestattet sein, Verbrechen im Cyber-Raum international zu verfolgen. Gleichzeitig soll der Staat mit geeigneten, anreizbasierten Mitteln dafür sorgen, dass Cyber-Vorfälle gemeldet werden. Dadurch ist er in der Lage, zu reagieren und Empfehlungen abzugeben. Im Verhältnis zwischen Staat und Unternehmen braucht es eine Kultur der Zusammenarbeit, nicht des Zwangs. Eine Meldung soll erfolgen, wenn ein Unternehmen dies wünscht, und in einer Art, die dem Unternehmen angemessen scheint. Durch die Förderung der Meldeerstattung sollen eine Erhöhung der Transparenz, eine bessere Erfassung der Bedrohungslage und eine Reduktion der Auswirkungen auf Dritte herbeigeführt werden.

Sensibilisierung von Bevölkerung, Unternehmen, Verwaltung und Politik
Cyber-Sicherheit ist eine klassische Verbundaufgabe und betrifft nicht nur Unternehmen und den Staat, sondern auch Private. Deshalb muss das Verständnis für Cyber-Risiken generell verbessert und Verhaltensänderungen müssen angeregt werden. Beispielsweise versenden Banken regelmässig

Informationen an ihre Kunden, um diese über Cyber-Angriffe zu informieren oder zwecks Warnung vor betrügerischen E-Mails oder Telefonanrufen.

Aus den lokalisierten Eckwerten und Handlungsfeldern ergeben sich die Ansprüche an Best Practices der Wirtschaft. So können allgemein anerkannte Standards im Bereich Datenverkehr ein Informationsgefälle zwischen den Parteien vermeiden, die Sicherheit des Datenverkehrs fördern und diesen beschleunigen. Dabei tragen sie zur Rechtssicherheit bei, ohne die Entwicklungen zu lähmen. Auch bei der Datenbearbeitung bringen Best Practices Vorteile für alle Beteiligten. Ein sich stetig entwickelnder Anonymisierungsstandard von Unternehmen kann gewährleisten, dass die Konzepte der Anonymisierung immer auf dem neusten Stand sind und somit der Persönlichkeitsschutz sichergestellt ist. Branchenspezifische Minimalstandards im Bereich Cybersecurity können ein flexibles, dezentrales System der Sicherheit im Cyber-Raum bewerkstelligen und vermeiden Asymmetrien. Ferner helfen Best Practices, ethische und technische Überlegungen in Verbindung mit Daten einzubringen und ersetzen in einer tauglichen Art und Weise einen absoluten gesetzlichen Anspruch auf Datenportabilität. Gesetzliche Regulierung, insbesondere solche auf Vorrat, wird durch die Anwendung von Best Practices in den dargestellten Handlungsfeldern überflüssig.

Fazit

Die technologische Entwicklung schreitet schnell voran. Die Schweiz muss dabei sicherstellen, auch weiterhin zu den Spitzenreitern zu gehören. Datenwirtschaft und zahlreiche sich daraus ergebende Anwendungsfelder von Sharing Economy bis hin zu künstlicher Intelligenz werden unser Wirtschaftsleben in Zukunft stark prägen. Dabei ist es von grundlegender Bedeutung, dass ein Ausgleich der Interessen derart stattfindet, dass das Vertrauen des Einzelnen geschützt und die Innovationskraft des Standorts nicht beschädigt wird.

Die Wirtschaft ist bereit, ihre diesbezügliche Verantwortung wahrzunehmen. Dabei legt sie dar, mit welchen Instrumenten das Vertrauen in unsere Unternehmen gesichert werden kann und gleichzeitig die Schweiz im internationalen Wettbewerb die notwendigen Mittel in den Händen hält, um weiterhin an vorderster Front am Fortschritt teilzunehmen. Entscheidend ist, dass nicht mit starren Regeln mögliche Entwicklungen abgeklemmt oder gar verhindert werden. Wie dies im Spannungsfeld der Interessen geht, zeigt die vorliegende Datenpolitik der Wirtschaft auf.

Grafik 6

Die Eckwerte, Handlungsfelder und Forderungen dienen als Basis für die Entwicklung eines Grundbekenntnisses der Wirtschaft.

Best Practices als Lösung für eine Datenpolitik

Quelle: eigene Darstellung
www.economiesuisse.ch

Dank

Besonderer Dank gilt den Mitgliedern der Arbeitsgruppe Datenpolitik von economiesuisse und repräsentierend für die zahlreichen Teilnehmenden in den verschiedenen Untergruppen den folgenden Personen, die für die Leitung der Untergruppen verantwortlich waren:

- Dr. Matthias Bossardt, Leiter Cybersecurity KPMG Schweiz, KPMG AG, Leiter der Sub-Arbeitsgruppe Cybersecurity in der AG Datenpolitik von economiesuisse
- Maria Chiara Atzori, Head Data Privacy CH, Novartis International AG, Leiterin der Sub-Arbeitsgruppe Informationelle Selbstbestimmung & Big Data der AG Datenpolitik von economiesuisse
- Werner W. Wyss, Head Regulatory Affairs, Zürcher Kantonalbank, Leiter der Sub-Arbeitsgruppe Datenverkehr in der AG Datenpolitik von economiesuisse
- Gema Olivar Pascual, Designated General Counsel, PricewaterhouseCoopers AG, Leiterin der Sub-Arbeitsgruppe Daten & Algorithmen als Rechtsobjekte in der AG Datenpolitik von economiesuisse
- Jean-Marc Hensch, Geschäftsführer, swico, Leiter der Sub-Arbeitsgruppe Zugangs- und Nutzungsrechte in der AG Datenpolitik von economiesuisse
- Nadine Büchler, wissenschaftliche Mitarbeiterin Wettbewerb & Regulatorisches bei economiesuisse, Sekretärin und Koordinatorin der AG Datenpolitik bis September 2017

Ivette Djonova

Projektleiterin Wettbewerb & Regulatorisches

Erich Herzog

Bereichsleiter Wettbewerb & Regulatorisches, General Counsel, Mitglied der erweiterten Geschäftsleitung

1. Die economiesuisse-Publikation «Digitale Wirtschaft» zeigt auf, was die Schweiz tun muss, um zu den Gewinnern der durch technologische Entwicklung verursachten Veränderungen zu gehören: economiesuisse/W.I.R.E., Zukunft digitale Schweiz, Wirtschaft und Gesellschaft weiterdenken, August 2017

2. Im Zentrum der Digitalisierung steht die Möglichkeit, Daten zu generieren, diese zu verarbeiten, zu speichern und zu übermitteln: für Details siehe economiesuisse/W.I.R.E., Zukunft digitale Schweiz, a.a.O., S. 14 ff.

3. Blockchain: Die Datenbanktechnologie Blockchain ist ein dezentrales Verfahren zum Speichern und Verschlüsseln von Daten. Sie basiert auf einer stetig wachsenden Liste von aufeinander basierenden Datensätzen. Einmal gespeicherte Daten können zwar ausgelesen, aber nicht mehr verändert werden. Die Blockchain zeichnet sich durch die Manipulationsresistenz aus.

4. In solchen Fällen kann eine Regelung der Rechte an Daten ausnahmsweise sinnvoll sein.-: Parlamentarische Initiative 17.410 M. Dobler: «Daten sind das höchste Gut privater Unternehmen, Datenherausgabe beim Konkurs von Providern regeln

5. In Europa wurden die Regeln unlängst verschärft, mit direkten Auswirkungen auf die Schweiz-: Datenschutz-Grundverordnung der EU (DSGVO) mit Inkrafttreten am 25. Mai 2018; von der Schweiz ratifizierte Datenschutzkonvention 108 des Europarats

6. Big-Data-Analysen: Big Data ist ein Sammelbegriff für verschiedene Technologien, um grosse Mengen von Daten zu erheben und/oder auszuwerten. Die Datenmengen sind zu gross, zu komplex oder verändern sich zu schnell oder sind zu unstrukturiert, um sie mit gewöhnlichen Methoden der Datenverarbeitung bewältigen zu können