Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Stand: 15. Oktober 2019

Bericht zu den Empfehlungen der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit:

Kenntnisnahme und weiteres Vorgehen

Inhalt

1 Zusammenfassung

Der Bundesrat hat am 5. September 2018 den Schlussbericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit zur Kenntnis genommen und das UVEK beauftragt, in Zusammenarbeit mit allen betroffenen Departementen bis Mitte 2019 den Bericht und insbesondere die 51 Handlungsempfehlungen der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» zu analysieren und dem Bundesrat 2019 allfällige Folgearbeiten zum Entscheid zu unterbreiten. Der Bericht wurden von einer interdisziplinären Expertengruppe unter dem Präsidium von Alt Nationalrätin Brigitta Gadient erstellt.

Die 51 Empfehlungen der Expertengruppe werden mehrheitlich (31) angenommen. Häufig decken sich die Expertenempfehlungen mit bereits laufenden Aktivitäten oder Vorhaben.

19 Empfehlungen sollen zum gegenwärtigen Zeitpunkt nicht weiterverfolgt werden. Gründe dafür sind insbesondere fehlende Zuständigkeiten des Bundes, hoheitliche Zuständigkeiten der Kantone, Städte und Gemeinden oder bereits publizierte, den entsprechenden Empfehlungen zuwiderlaufende Positionen des Bundesrates bzw. des Parlaments zum jeweiligen Thema.

Bei einer Empfehlung laufen Abklärungen, deren Ergebnisse zu einer Annahme oder Ablehnung führen können.

Bei folgenden Empfehlungen besteht zusätzlicher Handlungsbedarf, der jeweils in geeignetem Rahmen weiterzuverfolgen ist:

- **Digitale Verträge und Inhalte: Prüfung unter Berücksichtigung der internationalen Entwicklungen, ob Anpassungen im Vertragsrecht nötig sind**.
- Prüfung der Ausgestaltung eines **Zwangslizenzen-Systems mit Blick auf den Zugang zu Sachdaten**.
- Erarbeitung von **auditierbaren IKT-Sicherheitsstandards** (durch Bund, Kantone, IKT-Fachverbände) und **Verpflichtung der Betreiber kritischer Infrastrukturen**, diese Sicherheitsstandards zu beachten.

Der vorliegende Bericht des UVEK gibt die Rückmeldungen der Departemente zu den jeweils inhaltlich von ihnen verantworteten Themen wieder.

2 Einleitung

Der Bundesrat hat am 5. September 2018 den Schlussbericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit zur Kenntnis genommen.[1] Der Bericht wurde von einer interdisziplinären Expertengruppe mit Vertretern aus Wissenschaft, Wirtschaft und Verwaltung in dreijähriger Arbeit erstellt. Die Expertengruppe geht auf die Motion 13.3841 von Ständerat Paul Rechsteiner zurück und wurde von alt Nationalrätin Brigitta Gadient präsidiert. Das Ergebnis ist ein über 190-seitiger Bericht mit 51 Empfehlungen zu unterschiedlichen Gebieten, welche die Datenbearbeitung und Datensicherheit betreffen. Das UVEK wurde am 5. September 2018 vom Bundesrat beauftragt, in Zusammenarbeit mit allen betroffenen Departementen bis Mitte 2019 den Bericht und insbesondere die 51 Handlungsempfehlungen der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» zu analysieren und dem Bundesrat 2019 allfällige Folgearbeiten zum Entscheid zu unterbreiten.

Die Empfehlungen der Expertengruppe richten sich mehrheitlich an den Bund, z.T. auch an Kantone und Gemeinden. Die Geschäftsstelle Digitale Schweiz GDS, angesiedelt im Bundesamt für Kommunikation, lancierte im Dezember 2018 eine Umfrage bei den Departementen und der BK zu den Expertenempfehlungen. Sie sollten mitteilen, ob sie die sie betreffenden Empfehlungen annehmen oder ablehnen und welche Empfehlungen aus ihrer Sicht prioritär zu behandeln seien. Im Ablehnungsfall waren sie gebeten, einen Grund anzugeben. Der vorliegende Bericht gibt eine Übersicht über die Rückmeldungen der Departemente und der BK.

3 Rückmeldungen der Bundesverwaltung zu den Empfehlungen

Die 51 Empfehlungen der Expertengruppe werden mehrheitlich (32) angenommen. Häufig decken sich dabei die Expertenempfehlungen mit bereits laufenden Aktivitäten oder Vorhaben. Abgelehnt werden 18 Empfehlungen. Gründe hierfür sind insbesondere eine fehlende Zuständigkeit des Bundes, eine hoheitliche Zuständigkeit bei Kantonen und Gemeinden oder eine dezidiert andere publizierte Auffassung des Bundesrates bzw. des Parlaments zum jeweiligen Thema. Bei einer Empfehlung (Nr. 39, Innovation partizipative Demokratie) laufen entsprechende Arbeiten, deren Ergebnisse letztlich zu einer Annahme oder Ablehnung führen können Die Nummerierung der Empfehlungen im Folgenden widerspiegelt keine Priorisierung, sondern die Reihenfolge der Themen im Bericht der Expertengruppe.

Folgende Themen werden von der Bundesverwaltung angenommen, wobei zu ihrer Umsetzung zusätzlicher Handlungsbedarf besteht, der im jeweils geeigneten Rahmen weiterzuverfolgen ist:

- Empfehlung Nr. 15: Der Bund prüft für digitale Verträge und Inhalte unter Berücksichtigung der internationalen Entwicklungen, ob Anpassungen im Vertragsrecht nötig sind: Wenn die entsprechenden Arbeiten in der EU vorliegen und die Diskussionen dort abgeschlossen sind, erscheint es sinnvoll zu prüfen, ob in der Schweiz allenfalls Handlungsbedarf besteht.

- Empfehlung Nr. 20: Der Bund prüft die Ausgestaltung eines Zwangslizenzen-Systems mit Blick auf den Zugang zu Sachdaten.

- Empfehlung Nr. 25: Bund und Kantone erarbeiten in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards und verpflichten die Betreiber kritischer Infrastrukturen, diese Sicherheitsstandards zu beachten.

[1] https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-72083.html

3.1 Angenommene Empfehlungen der Expertengruppe

Nr. 2: Der Bund stellt in Zusammenarbeit mit den Kantonen sicher, dass die eingesetzte Verschlüsselungstechnik bei sensitiven Daten auch langfristig die notwendige Informationssicherheit gewährleistet. Die entsprechende Verschlüsselungstechnik soll allen privaten und öffentlichen Nutzerinnen und Nutzern zur Verfügung gestellt werden.

Zuständig: VBS, EFD

Rückmeldung VBS: Teilweise Annahme, Priorität hoch, Aktivität läuft
Rückmeldung EFD: Teilweise Annahme

VBS: Bei der Führungsunterstützungsbasis FUB des VBS ist die kryptologische Fachstelle des Bundes angesiedelt. Diese sorgt mit ihren kryptologischen Prüfungen und Empfehlungen dafür, dass bei sensitiven Daten kryptografisch sichere Systeme beschafft werden. Sie berücksichtigt dabei mögliche zukünftige Bedrohungen sowie die kryptologische Forschung und kryptografische Entwicklungen. Die Fachstelle kann bei Bedarf auch Kantone und Betreiber von kritischen Infrastrukturen beraten. Sie war bei der Erstellung des Berichtes nicht Teil der Expertengruppe, das dort vorhandene Wissen ist nicht in den Bericht eingeflossen.

Für einen hohen Schutzbedarf kommen im Bund bereits heute praxiserprobte Lösungen nach aktuellem Stand der Technik und Forschung zum Einsatz. Im Falle von neuen Anforderungen unterstützt die Fachstelle für Kryptologie in enger Kooperation mit Hochschulen und Industrie bei Design und Entwicklung sicherer Kryptobausteine.

Die Empfehlung für ein sicheres und hoch verfügbares Kommunikationsnetzwerk (s. auch Empfehlung Nr. 3) setzt kryptografisch abgesicherte Kommunikationsinfrastrukturen voraus. Bei den symmetrischen Verschlüsselungsverfahren ist in den letzten Jahren zum Schutz gegen Quantencomputer-Angriffe die Schlüssellänge auf 256 Bit erhöht worden. Die heute aktuellen asymmetrischen Verfahren wären in 10 bis 15 Jahren bei der Realisierung eines entsprechend grossen Quantencomputers nicht mehr sicher. Dieses Problem betrifft jedoch die ganze Welt und nicht nur die Schweiz. Dementsprechend wird weltweit an der Realisierung und Implementierung von Quantencomputer-sicheren asymmetrischen Verfahren gearbeitet. Die Wahrscheinlichkeit dafür, dass in 5 Jahren z.B. neue Smartcard-Technologien vorliegen, welche diese neuen asymmetrischen Verfahren anwenden können, ist um Faktoren grösser als diejenige eines Quantencomputers in 10 bis 15 Jahren, der die heute gängigen asymmetrischen Verfahren brechen könnte. Zudem ist FUB Kryptologie schon länger darauf bedacht, dass zum Schutz von strategischen Langzeitgeheimnissen nur symmetrische Verfahren mit grosser Schlüssellänge eingesetzt werden.

EFD und VBS: Nicht weiterverfolgt wird momentan der zweite Teil der Empfehlung «Die entsprechende Verschlüsselungstechnik soll allen privaten und öffentlichen Nutzerinnen und Nutzern zur Verfügung gestellt werden». Eine breite «Zur-Verfügung-Stellung» derartiger Technologien für private und öffentliche Nutzerinnen und Nutzer ist nicht einfach. Zum einen müsste eine aufwändige Infrastruktur zur Bearbeitung von Rückfragen (Help-Desk) aufgebaut und betrieben werden. Zum anderen sind solche Verschlüsselungs-Technologien nur dann sinnvoll, wenn sie in eine gegebene IKT-Infrastruktur integriert werden können. Das ist beispielsweise auf den Heimcomputern von privaten Nutzerinnen und Nutzern oft nicht möglich. Zudem kann man sich streiten, ob es überhaupt sinnvoll ist, Verschlüsselungstechnik auf nicht vertrauenswürdigen IKT-Systemen (wie eben Heimcomputern) einzusetzen, weil diese damit beliebig unterlaufen werden kann.

Letztlich stellen sich hier ebenfalls wettbewerbstechnische, ordnungspolitische und beschaffungsrechtliche Fragen. So gibt es für eine breite «Zur-Verfügung-Stellung» von Verschlüsselungstechnologien und entsprechenden Lösungen weder eine rechtliche Grundlage noch einen gesetzlichen Auftrag. Diese müssten vorgängig zuerst geschaffen werden.

Nr. 3: Der Bund prüft in Zusammenarbeit mit den Kantonen die Möglichkeiten, privaten und öffentlichen Nutzerinnen und Nutzern ein sicheres und hoch verfügbares Kommunikationsnetzwerk zur Verfügung zu stellen.

Zuständig: EFD, UVEK, VBS

Rückmeldung EFD: Annahme, nicht dringend, wichtig
Rückmeldung UVEK: Annahme
Rückmeldung VBS: Annahme, Aktivitäten laufen

EFD: Der Bundesrat hat am 21. November 2018 die Botschaft zu einem Verpflichtungskredit für ein nationales sicheres Datenverbundsystem verabschiedet. Mit dem Vorhaben soll ein krisensicheres Kommunikationssystem für Bund und Kantone geschaffen werden. Davon zu trennen ist jedoch die Zurverfügungstellung eines sicheren und hoch verfügbaren Kommunikationsnetzwerks für die private Nutzung. Diese sollte über geeignete Auflagen und Vorgaben an die Fernmeldedienstеanbieterinnen sichergestellt werden. Denn der Bericht suggeriert, dass morgen die Netzleistung eine Bundesaufgabe wäre, und dies sollte wie bis anhin der Privatwirtschaft überlassen sein.

Annahme der Empfehlung, nicht dringend, da langer Zeithorizont; wichtig.

UVEK: Der Verweis im Bericht auf die SCION-Technologie (SCION steht für Scalability, Control and Isolation on Next Generation Networks) erscheint prüfenswert[2]. Dies könnte eine Aufgabe für den oder die neu einzusetzende/n Delegierte/n für Cybersicherheit («Mr Cyber / Mrs Cyber») sein und sollte im Umfeld des Cyber-Kompetenzzentrums an die Hand genommen werden. Eine Absprache mit den Fernmeldedienstеanbieterinnen ist hierbei zentral.

VBS: Das Führungsnetz Schweiz soll nicht nur der Armee zur Verfügung stehen, sondern auch zivilen Organisationen mit sicherheitsrelevanten Aufgaben, wie die FUB erläutert. Diesbezüglich laufen Gespräche mit dem Sicherheitsverbund Schweiz (SVS), der alle Organisationen und Mittel, mit denen die Schweiz auf sicherheitspolitische Bedrohungen und Gefahren reagieren kann, umfasst. Die IKT-Teilstrategie Verteidigung 2012 - 2025 sieht vor, dass die Sicherheit der IKT-Infrastrukturen auf die neuen Bedrohungen ausgerichtet ist. Wenn es die Topologie zulässt, wird das Führungsnetz Schweiz mitbenutzt.

Für Bund und Kantone wird ein Sicheres Datenverbundsystem Schweiz mit den folgenden Teilen geschaffen: SDVN (SicheresDatenVerbundNetz); DZG (DatenZugangsSystem Polydata); LVS (LageVerbundSystem). Das bisherige Meldevermittlungssystem Vulpus soll abgelöst werden.

Aus sicherheitspolitischer Sicht sollte in Zusammenarbeit mit dem WBF auf behördlicher Seite und den Hochschulen auf wissenschaftlicher/technischer Seite das Projekt SCION weiter beobachtet, bei Bedarf unterstützt und weiterentwickelt werden (SCION steht für Scalability, Control and Isolation on Next Generation Networks: mehr Sicherheit im Internet, Routenkontrolle, Ausfallisolierung gegen Routenfehler und Fehlkonfigurationen und explizite Vertrauensinformationen für die Ende-zu-Ende-Kommunikation).

Zahlreiche Leistungen im öffentlichen, privaten und technischen Bereich sind vom weltumspannenden Internet abhängig. Bei einem Grossangriff auf das Internet ist heute eine schweizweite "Internetsouveränität" nicht sichergestellt. Sender und Empfänger haben im klassischen Internet keine Kontrolle über die Transportwege. Es wäre zu klären, welche Leistungen unser Land bei der aktuell hohen Vernetzungsdichte ohne das Internet noch erbringen kann (z.B. SAP-Support, Bestellung von Hardwarekomponenten, Software, etc.)? Vertiefte Kenntnisse der Lieferantenketten werden unabdingbar (Lieferanten von Hardware, Software, Informationen, Wissen, ...). --> IST-Bild

---

[2] Expertenbericht «Zukunft der Datenbearbeitung und Datensicherheit», S. 57.

Nr. 4: Der Bund prüft in Abstimmung mit der Entwicklung im Ausland, ob und in welchen Bereichen Standards und Zertifizierungen zu einer Voraussetzung für den Marktzugang von IKT-Komponenten erklärt werden müssen, und welche gesetzlichen Rahmenbedingungen dafür nötig sind.

Zuständig: EFD, UVEK, VBS

Rückmeldung EFD: Annahme; wichtig, nicht dringend
Rückmeldung UVEK: Annahme
Rückmeldung VBS: Annahme

EFD: Aufgabe des neu zu schaffenden Cyber-Kompetenzzentrums.

VBS: An dieser Stelle könnte armasuisse als Einkaufs- und Prüfstelle auftreten. Für Prüfungen und Zulassungen im kryptologischen Bereich ist die Fachstelle Kryptologie beizuziehen und dies in Abstimmung mit dem Cyber-Defence Campus von armasuisse. Wer ganz sichergehen will, kann die IKT-Sicherheit entlang seiner digitalisierten Prozesskette selber überprüfen (*supply chain security*).

Nr. 5: Der Bund schafft die notwendigen gesetzlichen Grundlagen für sichere staatlich anerkannte digitale Identitäten (für juristische und natürliche Personen sowie digitale Infrastrukturen).

Zuständig: EJPD; mitinteressiert: EDA

Rückmeldung EJPD: Teilweise Annahme

EJPD: Die Empfehlung kann insofern angenommen werden, als eine digitale Identität nur für natürliche Personen möglich ist. Genau dies sieht auch das E-ID-Gesetz vor. Juristische Personen haben auch in der analogen Welt keine eigene persönliche Identität, da ihr Handeln immer durch natürliche Personen induziert wird. Sie können identifiziert werden, sei dies durch einen HR-Eintrag oder einen Eintrag im UID-Register, sie können aber nicht losgelöst von natürlichen Personen handeln. Jede juristische Person in der Schweiz verfügt heute über eine UID-Nummer, die sie «identifiziert», eine Art digitalen Ausweis kann aber nicht erstellt werden. Bei digitalen Infrastrukturen ist dies noch viel weniger möglich, auch analoge Infrastrukturen haben keine eigene Identität. Auch sie können nur mit Attributen beschrieben und allenfalls in Verzeichnisse aufgenommen werden.

EDA: Es ist sicherzustellen, dass auch die Bedürfnisse der Auslandsschweizerinnen und –schweizer berücksichtigt werden, die von Dienstleistungen in der Schweiz ebenfalls profitieren.

Nr. 6: Der Bund prüft die Möglichkeit, soweit Identifizierungen nicht notwendig sind, anonyme Anmeldenachweise („anonymous Credentials“) einzuführen, insbesondere für die Beziehungen zwischen Privaten und Behörden, aber auch als Mittel für die Online-Nutzer.

Zuständig: EFD, EDA

EFD: Annahme
EDA: Annahme

EDA: Das EDA begrüsst die Empfehlung «Der Bund prüft die Möglichkeit, soweit Identifizierungen nicht notwendig sind, anonyme Anmeldenachweise („anonymous Credentials“) einzuführen, insbesondere für die Beziehungen zwischen Privaten und Behörden, aber auch als Mittel für die Online-Nutzer». Dies aus folgendem Grund: Die konsularischen Dienstleistungen unterliegen einem steten und starken Wandel. Die KD gestaltet diesen Wandel mit ihrem langfristigen Projekt «Weiterentwicklung Konsularische Dienstleistungen» aktiv mit, das parallel und in Ergänzung zu AVIS28 läuft. Viele Berei-

che in diesem Projekt betreffen den digitalen Behördenverkehr, digitale Auskunftsvermittlung etc. Dabei wird es vermutlich nicht in jedem Fall nötig sein, dass die Behörden die *ganze* Identität der Benutzerinnen und Benutzer kennen – es kann je nach Dienstleistung auch ausreichend sein, nur eine zwingend notwendige Information zu kennen, beispielsweise die Staatsbürgerschaft des Kunden, der eine Visainformation einholt. Diese Möglichkeit bieten nach unserem Verständnis «anonyme Anmeldenachweise».

Nr. 7: Der Bund sorgt für die Schaffung eines nationalen Netzwerks zur Förderung der Forschung im Bereich der digitalen Transformation mit Schwerpunkt Informationssicherheit und des Wissenstransfers zwischen der Forschung und der Wirtschaft.

Zuständig: WBF, ETH-Rat, innosuisse, Mitinteresse VBS

Rückmeldung WBF: Annahme
Rückmeldung VBS: Annahme

WBF: Der Schweizerischer Nationalfonds (SNF) hat im Auftrag des Bundesrates soeben das «Nationale Forschungsprogramm (NFP) 77 "Digitale Transformation"» initiiert. Es will die Wirkungszusammenhänge sowie die konkreten Auswirkungen der digitalen Transformation in der Schweiz untersuchen. Die drei Schwerpunkte des Programmes sind Bildung und Lernen, Ethik, Vertrauenswürdigkeit und Governance sowie Wirtschaft und Arbeitsmarkt. Es dauert 5 Jahre und verfügt über einen Finanzrahmen von CHF 30 Millionen.

Weiter unterstützt Innosuisse nationale thematische Netzwerke (NTN) mit dem Ziel, den Wissens- und Technologietransfer anzukurbeln. Insbesondere eines der aktuell zehn Netzwerke – Swiss Alliance for Data-intensive Services (data+services) - setzt sich für die Förderung der Zusammenarbeit innovativer Firmen und Hochschulen ein, welche ihr Wissen aus spezifisch datenrelevanten Bereichen wie Informationstechnologie, Künstlicher Intelligenz, Wirtschaft und Psychologie kombinieren und zu marktfähigen Produkten und Dienstleistungen weiterentwickeln.

VBS: Im Rahmen des Aktionsplans Cyber-Defence des VBS laufen bereits Aktivitäten im Sinne der Expertenempfehlung. Im Aufbau ist der Cyber-Defence Campus bei armasuisse W+T mit den zwei zusätzlichen Standorten ETHZ (Q3-2019) und EPFL (Q2-2019). Zusammenarbeit mit Forschungspartnern, der Industrie und Leistungserbringern ist im Cyber-Defence Campus verankert. Der Cyber-Defence Campus baut ein nationales Forschungsnetzwerk im Bereich Cyber-Defence auf.

Nr. 8: Der Bund setzt sich für eine Stärkung der informationellen Selbstbestimmung ein, fördert namentlich datenschutzfreundliche Technologien und prüft unter Berücksichtigung der internationalen Entwicklungen und des technischen Fortschritts ergänzende und alternative Ansätze inner- und ausserhalb des Datenschutzrechts.

Zuständig: EJPD, EDÖB, EDA

Rückmeldung EJPD/BJ: Annahme
Rückmeldung EDÖB: Annahme

EJPD: Diese Empfehlung betrifft eine Daueraufgabe, welche das BJ bereits wahrnimmt. Der Empfehlung wird in weiten Teilen im Rahmen der Totalrevision des Datenschutzgesetzes Rechnung getragen. Im Entwurf des Bundesrates (E-DSG) sind unter anderem der Grundsatz des Datenschutzes durch Technik («Privacy by Design»), die Förderung der Selbstregulierung im Bereich des Datenschutzes durch branchenweite Verhaltenskodizes und (freiwillige) Zertifizierung sowie die Erhöhung der Transparenz von Datenbearbeitungen vorgesehen. Dabei berücksichtigt der E-DSG insbesondere die Entwicklungen in der EU und im Europarat. Der Bundesrat will sicherstellen, dass die Schweiz die modernisierte Datenschutz-Konvention SEV 108 des Europarates sobald als möglich ratifizieren kann.

Ausserdem werden die internationalen Entwicklungen im Bereich der künstlichen Intelligenz aufmerksam von einer bundesverwaltungsinternen Arbeitsgruppe verfolgt.

Allerdings ist darauf hinzuweisen, dass wir nicht alle im Bericht der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» vorgeschlagenen «ergänzenden Massnahmen im Rahmen des traditionellen Datenschutzes» unterstützen bzw. nachvollziehen können. Insbesondere die im Rahmen des «Sandboxing-Ansatzes» vorgeschlagene Lockerung des Zweckbindungsgrundsatzes erscheint uns aus datenschutzrechtlicher Sicht problematisch.

EDÖB: Der EDÖB begrüsst die im E-DSG vorgeschlagenen neuen Instrumente, welche die Entwicklungen in der EU und im Europarat berücksichtigen. Der EDÖB findet es wichtig, dass die modernisierte Datenschutz-Konvention SEV 108 des Europarates sobald als möglich unterzeichnet und ratifiziert wird. Auch die im der europäischen Datenschutzgesetzgebung vorgesehene Datenportabilität müsste ins neue DSG aufgenommen werden.

Nr. 10: Bund und Kantone passen die Ausstattung der Datenschutzbehörden mit Befugnissen und Mitteln so an, dass diese es ihnen ermöglichen, ihre gesetzlichen Aufgaben der Sensibilisierung, Beratung und Aufsicht umfassend und wirkungsvoll wahrnehmen zu können.

Zuständig: EJPD, EDÖB

Rückmeldung EJPD: Teilweise Annahme
Rückmeldung EDÖB: Annahme

EJPD:

Bund: Dieser Empfehlung trägt der Bundesrat zu einem grossen Teil bereits in der Botschaft zur Totalrevision des DSG Rechnung. Zum einen werden im E-DSG die Kompetenzen des EDÖB gestärkt. Er erhält mehr Untersuchungsbefugnisse und soll inskünftig statt einer Empfehlung direkt verbindliche Verfügungen erlassen können (Art. 44 und 45 E-DSG). Allerdings sollen dem EDÖB nach Ansicht des Bundesrates (zumindest zum jetzigen Zeitpunkt) keine Sanktionskompetenzen zuerkannt werden (vgl. aber das Postulat 18.4100 der Staatspolitischen Kommission NR «Instrument der pekuniären Verwaltungssanktionen», welches der Bundesrat zur Annahme empfiehlt). Zum andern soll der EDÖB auch mehr Ressourcen erhalten. Da der E-DSG eine Reihe von Massnahmen einführt, die neue Aufgaben für den EDÖB mit sich bringen (z.B. Konsultation bei Datenschutz-Folgenabschätzungen), benötigt der EDÖB nach Ansicht des Bundesrates zusätzliche Personal- und Informatikressourcen. Gemäss der Botschaft zum E-DSG beträgt der zusätzliche Personalbedarf des EDÖB schätzungsweise zehn Stellen. Der Bundesrat schlägt vor, die Personalressourcen schrittweise zu gewähren und spätestens fünf Jahre nach Inkrafttreten des Gesetzes wieder zu evaluieren. Ein Teil der Personalressourcen soll durch Gebühren finanziert werden können. Ebenso sind gemäss der Botschaft zum E-DSG zusätzliche Informatikressourcen beim EDÖB erforderlich (BBl 2017 6941, 7177 ff.). Ein Teil dieser Ressourcen (zusätzlicher Personalbedarf von drei Stellen) soll dem EDÖB schon ab dem Jahr 2020 im Zusammenhang mit dem neuen Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen zugesprochen werden.

Kantone: Aufgrund der den Kantonen gemäss Bundesverfassung zukommenden Organisationsautonomie (Art. 47 Abs. 2 BV) fällt die «Ausstattung» der Datenschutzaufsichtsbehörde in ersten Linie in die kantonale Kompetenz. Der Handlungsspielraum des Bundes ist hier eingeschränkt. Mindestvorgaben für die Kantone ergeben sich aber aus Art. 37 DSG sowie aus dem geltenden Zusatzprotokoll zur Datenschutzkonvention SEV 108 des Europarates und der EU-Richtlinie 2016/680 für den Datenschutz in Strafsachen. Auch die (durch die Schweiz noch zu ratifizierende) modernisierte Datenschutzkonvention SEV 108 des Europarates verpflichtet die Kantone ihre Datenschutzaufsicht (soweit erforderlich) betreffend Kompetenzen und Ressourcen zu stärken.

EDÖB: In der Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 6941 ff.) wird ausdrücklich festgehalten, dass der EDÖB zusätzliches Personal braucht. Dies umso mehr, als der Beauftragte mit der exponentiell fortschreitenden Digitalisierung unabhängig von der Revisionsvorlage mit immer mehr Aufgaben betraut worden ist (vgl. S. 7176 der Botschaft). Der EDÖB selbst weist in seinem 26. Tätigkeitsbericht 2018/2019 darauf hin, dass die Kontrolldichte tief ist. Desgleichen wurde der Schweiz im Rahmen der Schengen Evaluation empfohlen, dem EDÖB ausreichende finanzielle und personelle Ressourcen zuweisen, damit er alle seine entsprechenden Aufgaben erfüllen kann. Zwar erhielt der EDÖB im Rahmen des am 1.3.2019 in Kraft getretenen Schengen-DSG drei zusätzliche Stellen. Es ist jedoch nicht gesichert, dass dem EDÖB die notwendigen Stellen für die Erfüllung der weiteren, im E-DSG vorgesehenen Aufgaben zugesprochen werden. Zudem ist das Schengen Datenschutzgesetz, welches dem EDÖB neue Aufgaben erteilt am 1. März 2019 in Kraft getreten, ohne dass gesichert ist, dass der EDÖB die dafür notwendigen zusätzlichen Stellen erhält. Unter diesen Voraussetzungen ist es für den EDÖB nicht möglich, seine Aufgaben umfassend wahrzunehmen und die vorgeschlagene Etappierung keineswegs angezeigt.

Nr. 11: Der Bund schafft in Zusammenarbeit mit den Kantonen Kooperationsformen zwischen den Datenschutzaufsichtsbehörden (z.B. Kompetenzzentrum).

Zuständig: EJPD, EDÖB

Rückmeldung EJPD: Annahme
Rückmeldung EDÖB: Annahme

EJPD: Wir weisen auf den Aufgabenkatalog des EDÖB gemäss Art. 52 E-DSG hin: Darin wird der EDÖB unter anderem beauftragt, mit den kantonalen Datenschutzbehörden zusammenzuarbeiten (Abs. 1 Bst. b).

EDÖB: Bereits heute besteht der Verein « privatim » (Verein der kantonalen Datenschutzaufsichtsstellen). Als assoziiertes Mitglied ist der EDÖB berechtigt, an den Bürositzungen mit beratender Stimme teilzunehmen.

Des Weiteren besteht eine Zusammenarbeit im Rahmen der Koordinationsgruppe der Schweizerischen Datenschutzbehörden im Rahmen der Schengen-Abkommen. Diese setzt sich aus je einem Vertreter der kantonalen Datenschutzbehörden sowie einem Vertreter des EDÖB zusammen, der ihr Sekretariat besorgt.

Nr. 12: Der Bund prüft mit Blick auf den Datenschutz und die Datensicherheit in Übereinstimmung mit den internationalen Entwicklungen und unter Berücksichtigung des Risikopotenzials und der Einsatzgebiete datenschutzkonforme Voreinstellungen.

Zuständig: EJPD, WBF, EDA

Rückmeldung EJPD: Annahme
Rückmeldung: WBF: Annahme
Rückmeldung EDA: Annahme

EJPD: Im Bereich des Datenschutzrechts wird diese Empfehlung durch die Totalrevision des DSG umgesetzt. Der Entwurf des Bundesrates verankert in Art. 6 E-DSG die Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen («Privacy by Design and by Default»). Ausserdem sieht der E-DSG in Art. 12 vor, dass die Hersteller von Datenbearbeitungssystemen oder -programmen sowie die für die Datenbearbeitung Verantwortlichen und Auftragsdatenbearbeiter ihre Systeme, Produkte und Dienstleistungen freiwillig zertifizieren lassen können. Nicht geregelt werden im E-DSG dagegen Marktzulassungsvoraussetzungen.

WBF: Dieses Prinzip ist in Art. 6 E-DSG vorgesehen. Zudem wird das Prinzip in der Schweiz offenbar heute bereits vielfach schon freiwillig umgesetzt.

EDA: Annahme der Empfehlung.

Nr. 15: Der Bund prüft für digitale Verträge und Inhalte unter Berücksichtigung der internationalen Entwicklungen, ob Anpassungen im Vertragsrecht nötig sind.

Zuständig: EJPD, EDA

Rückmeldung EJPD: Annahme
Rückmeldung EDA: Annahme

EJPD: Wenn die entsprechenden Arbeiten in der EU vorliegen und die Diskussionen dort abgeschlossen sind, erscheint es sinnvoll zu prüfen, ob in der Schweiz allenfalls Handlungsbedarf besteht.

Nr. 20: Der Bund prüft die Ausgestaltung eines Zwangslizenzen-Systems mit Blick auf den Zugang zu Sachdaten.

Zuständig: EJPD

Rückmeldung EJPD (IGE): Annahme

IGE: Der Zugang zu Sachdaten kann für KMU, Universitäten oder die Zivilgesellschaft komplex oder zu teuer sein. Darüber hinaus könnten einige Inhaber von sehr umfangreichen und voluminösen Datensammlungen ihre Marktposition missbrauchen. In diesen Situationen sind Hindernisse für den Zugang, die Nutzung und die Wiederverwendung von Daten Schranken für die wirtschaftliche, wissenschaftliche und soziale Entwicklung. Aus diesen Gründen hat die Europäische Kommission eine Reihe von Studien mit dem Titel « Data Economy Package for non-personal data » veröffentlicht, deren Ziel ist, einen freien Datenfluss von Sachdaten im Binnenmarkt zu gewährleisten. Diese wird manchmal als fast fünfte Grundfreiheit der Union wahrgenommen. Zu den Vorschlägen, die zur Gewährleistung eines freien Datenflusses geprüft wurden, gehört die Ausgestaltung eines Zwangslizenzen-Systems. Diese Rechtsinstitution ist sowohl im Immaterialgüter- als auch im Kartellrecht bekannt und deckt eine Vielzahl von Realitäten ab. Es handelt sich um ein heikles Thema, insbesondere im Hinblick auf das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS-Abkommen).

Ein System von Zwangslizenzen ist nicht die einzige Lösung, die von der Kommission angestrebt wird. So schlug sie insbesondere vor, eine Reihe von unverbindlichen Vertragsregeln für B2B-Verträge ("business to business") bei der Gewährung von Zugangs-, Nutzungs- und Wiederverwendungsrechten von Daten festzulegen oder eine Kultur der «open data» zu fördern. Das Problem stellt sich für die Schweiz in gleicher Weise wie für die Europäische Union. Mehrere von der Kommission aufgezeigte Lösungsansätze könnten für unser Land von Interesse sein. Wir empfehlen daher, dieses Mandat anzunehmen, sofern es neu formuliert wird, um einen breiteren Untersuchungsrahmen zu bieten: «Zugang zu Sachdaten: Analyse der aktuellen Situation und Aufzeigen von Lösungsoptionen». Dies wird es dem Mandat ermöglichen, auf den Ergebnissen der Arbeit der EU am «Data Economy Package for non-personal Data» aufzubauen und internationalen Entwicklungen Rechnung zu tragen.

Nr. 21: Der Bund ergänzt unter Berücksichtigung der internationalen Entwicklungen das Datenschutzrecht um das Element der Datenportabilität.

Zuständig: EJPD

Rückmeldung EJPD: Annahme

EJPD: (Vorbehalt: gemäss dem Auftrag des Bundesrates vom 9. Mai 2018). Das in der EU-Datenschutz-Grundverordnung 2016/679 enthaltene Recht auf Datenportabilität ist im Entwurf des Bundesrates zur Totalrevision des DSG nicht vorgesehen. Der Nationalrat hat sich jedoch in der Herbstsession 2019 für die Einführung eines derartigen Rechts aufgrund eines entsprechenden Vorschlags der vorbereitenden Kommission ausgesprochen. Bereits am 9. Mai 2018 hat der Bundesrat das BJ im Rahmen der Festlegung seiner Eckwerte für eine Datenpolitik der Schweiz damit beauftragt, den Regelungsbedarf zu einer sektor- bzw. branchenspezifischen Einführung der Datenportabiltät zu prüfen und bis spätestens Mitte 2020 allfällige Vorschläge für eine rechtliche Ausgestaltung zu unterbreiten.[3] Dieser Zeithorizont würde es auch erlauben, die ersten Erfahrungen innerhalb der EU mit dem Instrument der Datenportabilität sowie die Resultate der parlamentarischen Debatte zur Totalrevision des DSG zu berücksichtigen. Zunächst sit jedoch das Ergebnis der parlamentarischen Diskussionen zum E-DSG abzuwarten. Entgegen den Ausführungen im Bericht der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» sollten unserer Ansicht auch andere Lösungsmöglichkeiten als die Anknüpfung der Datenportabilität am datenschutzrechtlichen Auskunftsrecht in Betracht gezogen werden.

Nr. 25: Bund und Kantone erarbeiten in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards und verpflichten die Betreiber kritischer Infrastrukturen, diese Sicherheitsstandards zu beachten.

Zuständig: EFD, VBS, UVEK

Rückmeldung EFD: Annahme; dringend, wichtig
Rückmeldung VBS: Annahme; Aktivitäten laufen
Rückmeldung UVEK: Annahme

EFD, VBS, UVEK: Die Erarbeitung von überprüfbaren IKT-Sicherheitsstandards erfolgt über die im Umsetzungsplan der NCS definierten Projekte in enger Zusammenarbeit mit den Fachämtern. Für diese Arbeiten wird der Minimalstandard zur Verbesserung der IKT-Resilienz» des BWL aktiv miteinbezogen. Das Kompetenzzentrum-Cybersicherheit koordiniert die entsprechenden Arbeiten. Offen ist jedoch, wie die Betreiber kritischer Infrastrukturen zur Einhaltung dieser Standards verpflichtet werden, wie ein etwaiges Monitoring und die Aufsicht über die Einhaltung der Standards erfolgt. Hierfür sind unter Umständen neue sektorspezifische gesetzliche Grundlagen erforderlich.

Nr. 26: Der Bund baut ein Kompetenzzentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit) zu Fragen der Standardisierung im Bereich IKT-Sicherheit auf.

Zuständig: EFD, VBS

Rückmeldung EFD: Annahme; dringend, wichtig (keine Begründung)
Rückmeldung VBS: Annahme; Priorität hoch

VBS: Die vom Parlament angenommene Idee zur Schaffung eines Kompetenzzentrums sollte 2019 aufgebaut werden (basierend auf MELANI). Im Juni 2019 wurde der Delegierte Cyber-Sicherheit Bund ernannt.[4] Die gewählte Person rapportiert direkt dem Departementschef des EFD. Für CYD-VBS wird

[3] https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-70694.html

[4] https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-75421.html

eine enge Zusammenarbeit mit der neu geschaffenen Stelle wichtig sein. Somit können die Inhalte zur Umsetzung der bundesweiten Strategie optimal aufeinander abgestimmt werden.

Nr. 27: Der Bundesrat fördert in enger Zusammenarbeit mit den Dach- und Branchenverbänden, mit den Verbänden der IKT-Anbieter und mit interessierten Unternehmen Programme zur Verbesserung der Informationssicherheit in der Wirtschaft.

Zuständig: EFD, WBF

Rückmeldung EFD: Annahme; dringend, wichtig
Rückmeldung WBF: Keine

EFD: Die Verbesserung der Informationssicherheit in der Wirtschaft ist ein strategisches Ziel der NCS. Mit der Umsetzung der Massnahmen 8, 9, 13 und 29 soll dieses Ziel erreicht werden.

Nr. 28: Der Bund führt für die Betreiber kritischer Infrastrukturen eine Meldepflicht für Cybervorfälle ein. Er erarbeitet dabei zusammen mit den zuständigen Behörden, der Privatwirtschaft und den Verbänden die Grundlagen und berücksichtigt die internationale Entwicklung.

Zuständig: EFD, WBF, VBS, EDA

Rückmeldung EFD: Annahme, Aktivitäten laufen teilweise
Rückmeldung VBS: Annahme; Priorität hoch, Aktivitäten laufen teilweise
Rückmeldung EDA: Annahme
Rückmeldung WBF: Keine

EFD: Die betroffenen Regulatoren sollten ebenfalls zur Empfehlung befragt werden; Abklärungen laufen, s. Umsetzungsplan[5] zur Strategie der Schweiz zum Schutz von Cyberrisiken NCS.

VBS: Für die Erstellung des Bedrohungsbildes ist die Meldung von Cyber-Vorfällen wichtig. Meldungen erfolgen heute auf freiwilliger Basis. Die NCS behandelt diesen Aspekt mit der Massnahme 9 "Prüfung Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung." Die strategisch oder sicherheitspolitischen bedeutsamen Meldungen werden auf Stufe Kerngruppe Sicherheit und allenfalls Cyberaussschuss Bundesrat zu behandeln sein.

EDA: Das EDA ist in all den Fällen betroffen, die eine diplomatische, strategische oder sicherheitspolitische Komponente haben. Diese Fälle sind dann in der KGSi (und im SiA) zu behandeln, entsprechend müssen die KGSi-Ämter direkt in die Ausgestaltung der Meldepflicht involviert sein (im EDA die SIS als für die sicherheitspolitischen Gremien verantwortliche Stelle – die SIS zeigt sich dann verantwortlich für den EDA-internen Informationsaustausch, insbesondere mit dem Büro Cyber zu Tendenzen und Konsequenzen für die Aussen(sicherheits)politik der Schweiz und der DV für völkerrechtliche Fragen und Entwicklungen).

Ergänzende Rückmeldung EJPD/BJ: Wir weisen darauf hin, dass bei einer allfälligen Umsetzung der Empfehlung 28 auch die im E-DSG neu vorgesehene (allgemeine) Meldepflicht bei Verletzungen der Datensicherheit (Art. 22) berücksichtigt werden sollte: Besteht bei einer Verletzung der Datensicherheit (zum Begriff vgl. Art. 4 Bst. g E-DSG) voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen, muss der verantwortliche Datenbearbeiter inskünftig

[5] https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/umsetzungsplan.html; https://www.isb.admin.ch/isb/de/home/dokumentation/medienmitteilungen/newslist.msg-id-70482.html

so rasch als möglich eine Meldung an den EDÖB machen. Unter gewissen Umständen muss er zusätzlich auch die betroffenen Personen informieren, damit diese selber Massnahmen treffen können, um ihre Daten zu schützen.

Nr. 29: Der Bund sorgt in Zusammenarbeit mit den Kantonen, der Wirtschaft und den Forschungsinstituten dafür, dass mit dem Ausbau von MELANI ein landesweites Zentrum (bzw. eine Stelle im Rahmen eines Kompetenzzentrums für Cybersicherheit, s. Empfehlung 26) zur Prävention und Bewältigung von Cybervorfällen geschaffen wird.

Zuständig: EFD, EDA

Rückmeldung EFD: Annahme, Aktivitäten laufen
Rückmeldung EDA: Annahme

EDA: Das EDA (SIS) und/oder die KGSi ist zwingend einzubeziehen, um die Kongruenz zwischen sicherheitspolitischer Führung und den Gremien zur Cybersicherheit (insbesondere Fachstelle Cybersicherheit) sicherzustellen.

Nr. 31: Der Bund führt eine sicherheitspolitische Diskussion im Bereich Cybersicherheit darüber, ob und in welchem Umfang eigene Abwehrressourcen aufzubauen und/oder enge Kooperationen mit anderen Staaten einzugehen sind. Im Vordergrund soll dabei die Cyberresilienz stehen.

Zuständig: VBS, EDA

Rückmeldung VBS: Annahme, Aktivitäten laufen
Rückmeldung EDA: Annahme

VBS: Die geforderte sicherheitspolitische Diskussion im Bereich Cybersicherheit zu Cyberabwehr und allfälligen Kooperationsmöglichkeiten mit dem Ausland wird auf Stufe des vom Bundesrat neu geschaffenen Gremiums Cyberausschuss bzw. Kerngruppe Cyber (unter Einbezug des EDA) geführt werden müssen.

EDA: Im Berichtstext wird von der sicherheitspolitischen Diskussion und der Kooperation mit anderen Staaten gesprochen. Der Einbezug des EDA und der sicherheitspolitischen Führung (KGSi/SiA bzw. VBS, EJPD, EDA) in diese Diskussion ist zwingend (mindestens Vorbehandlung in KGSi und SiA) und kann nicht allein dem VBS überlassen werden.

Nr. 32: Der Bund trifft die nötigen Vorkehrungen, damit die Armee und die Militärverwaltung den zivilen Behörden subsidiär Mittel im Cyberbereich zur Verfügung stellen können. Diese sollen in ausserordentlichen Lagen die Betreiber kritischer Infrastrukturen unterstützen können.

Zuständig: VBS; Mitinteresse EFD

Rückmeldung VBS: Annahme, Aktivitäten laufen

VBS: Um ihren Auftrag jederzeit erfüllen zu können, muss die Armee ihre Informatiksysteme vor Cyberangriffen schützen. Damit sie über die notwendigen Instrumente zum Eigenschutz verfügt, hat der Bundesrat in seiner Sitzung vom 30. Januar 2019 mit einer neuen Verordnung[6] die Organisation und

[6] Verordnung über die militärische Cyberabwehr (MCAV) vom 30. Januar 2019, SR 510.921

die Zuständigkeiten für die Wahrung der militärischen Sicherheit im Cyberraum geregelt. Die Verordnung trat am 1. März 2019 in Kraft. Die Armee hat jedoch keine Gesamtverantwortung im Bereich Cyber für die Schweiz und erhält mit dieser Verordnung keine über den Eigenschutz und die Selbstverteidigung hinausgehenden Zuständigkeiten. Die Verordnung zeigt aber im Detail auf, wie die Schweizer Armee den Eigenschutz und die Selbstverteidigung im Cyberraum wahrnimmt. Sie regelt auch die Aufgaben des Bundesrates sowie der Chefin des VBS und enthält Ausführungsbestimmungen im Bereich Einsatz und Ausbildung sowie Forschung.

Aus der Motion Dittli 17.3507[7], die im März 2018 angenommen wurde, sind zum Thema folgende zwei Punkte zu erwähnen:

- die Betreiber kritischer Infrastrukturen subsidiär unterstützen;
- die zivilen Behörden des Bundes und der Kantone bei Cyberangelegenheiten subsidiär unterstützen.

Die NCS-Massnahme 24 fordert eine Gewährleistung der Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden.

EFD: Eine Absprache mit dem Cyber-Kompetenzzentrum ist nötig

Nr. 33: Der Bund präzisiert die Kriterien für den verhältnismässigen Einsatz der Armee im Cyberbereich.

Zuständig: VBS, EDA

Rückmeldung VBS: Annahme, Aktivitäten laufen
Rückmeldung EDA: Annahme

VBS: Wird von der Stelle CYD VBS in Zusammenarbeit mit der FUB im Rahmen des Aktionsplans Cyber-Defence VBS behandelt.

EDA: Verhältnismässiger Einsatz der Armee im Cyberbereich. Der Einsatz der Armee im Cyberbereich ist immer auch ein Einsatz im internationalen (Cyber-)Raum. Die sicherheits- und aussenpolitische/diplomatische Komponente erfordert einen direkten Einbezug des EDA (DV, ASP/SIS)

Nr. 35: Bund und Kantone schaffen für die digitale Transformation im Bereich der Behördentätigkeiten medienbruchfreie und einheitliche Rahmenbedingungen, die eine auch für Private und Wirtschaft möglichst benutzerfreundliche sowie gut koordinierte und vernetzte Datenbearbeitung unter Wahrung des Datenschutzes ermöglichen und, wo es sinnvoll erscheint, Lösungen schweizweit skalieren lassen.

Zuständig: EFD, Mitinteresse EDA

Rückmeldung EFD: Annahme

EFD: Umsetzung der Tallinn-Erklärung mit dem Once-only-Prinzip

[7] Motion 17.3507 Dittli Josef vom 15.06.2017 Ein Cyberdefencekommando mit Cybertruppen für die Schweizer Armee, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507

EDA: Entspricht den EDA-internen Grundsätzen für eine "*Seamless customer journey*" und den Arbeiten an den entsprechenden Webseiten des Departements.

Nr. 36: Bund und Kantone stellen sicher, dass bei der Umsetzung der E-Government-Strategie Schweiz die Bevölkerungsgruppe der „Offliner“ durch die Digitalisierung nicht gesellschaftlich ausgegrenzt wird.

Zuständig: EFD, Mitinteresse EDA

Rückmeldung EFD: Annahme
Rückmeldung EDA: Annahme

EFD: Das Prinzip des Bundes ist "digital-first" und nicht "digital-only". Hierzu müssen zwingend auch Kosten-Nutzen Überlegungen einfliessen: Was würde es kosten, diese Offliner einzubinden?

EDA: Diese Empfehlung betrifft auch die Auslandsschweizerinnen und –schweizer sowie Reisende in der Schweiz.

Nr. 37: Bund und Kantone schaffen die gesetzlichen Voraussetzungen, damit die mit öffentlichen Mitteln erhobenen Daten unter Wahrung der datenschutzrechtlichen Vorgaben für die weitere Verwendung erschlossen werden können.

Zuständig: EDI

Rückmeldung EDI /GS: Annahme

EDI: Im Rahmen der Umsetzung der Open Government Data Strategie 2019-2023[8] hat das EDI den Auftrag erhalten, bis Mitte 2020 abzuklären, welche rechtlich-organisatorischen Massnahmen notwendig sein können, um verbindlichere und nach Möglichkeit optimale Rahmenbedingungen für den Ausbau von OGD im Sinne der Strategie bereitzustellen (Grundsätze 4.2.3). Neben der Prüfung allfälliger Rechtssetzungsvorgaben zu diesem Zweck werden u.a. auch die Einführung international etablierter Nutzungsbedingungen geprüft (siehe Massnahme 1) und ein laufendes Monitoring der Qualitätsanforderungen eingeführt (siehe Massnahme 2). Die Stellen der zentralen Bundesverwaltung sind darüber hinaus gemäss Strategie bereits ab 2020 verpflichtet, ihre neuen Daten grundsätzlich, sofern keine legitimen Schutzinteressen oder rechtlichen Bestimmungen entgegenstehen, als OGD zu publizieren. Die Kantone werden dazu eingeladen, u.a. in einem Forum «Öffentliche Verwaltungen», die Strategie und die entwickelten rechtlichen Lösungen in enger Zusammenarbeit mitumzusetzen.

Nr. 38: Bund und Kantone richten eine Fachstelle ein, die Standardisierungen und Normierungen auf der technischen und operativen Ebene bei der Datenbearbeitung im Bereich OGD erarbeitet und alle betroffenen Verwaltungsstellen fachlich unterstützt.

Zuständig: EDI

Rückmeldung EDI /GS: Annahme der Federführung für die Umsetzung

EDI: Die Open Government Data Strategie 2019-2023 hat das EDI mit der Gesamtleitung der Umsetzungsarbeiten betraut und darunter als eine Massnahme die Einrichtung einer «Geschäftsstelle Open Government Data» im Departement, im Bundesamt für Statistik BFS, definiert (Grundsätze 4.2.1, Ziele 4.3.1-5, Ressourcen 6.2). Die Geschäftsstelle im BFS hat per 1.1.2019 ihre Arbeit aufgenommen und

[8] Strategie für offene Verwaltungsdaten in der Schweiz 2019–2023 (Open-Government-Data-Strategie, OGD-Strategie)

koordiniert die Massnahmen der Strategie in Bezug auf die praktische Umsetzung. Darunter sind selbstverständlich alle Fragen der Standardisierung und Normierung, wie sie im Massnahmenplan im Anhang der Strategie vorgesehen (z.B. die Massnahmen zur Standarisierung und Qualität von publizierten OGD-Daten (Massnahme 2), oder technische-operative Synergien (Massnahme 3).

Die OGD-Geschäftsstelle des Bundes ist als Fachstelle mit den äquivalenten und inzwischen vielfach eingerichteten Stellen auf kantonaler Ebene direkt vernetzt und entwickelt die Themen wie Standardisierung und Normierung gemeinsam weiter. Hierzu werden wie in der Strategie vorgesehen (Organisation 6.1) entsprechende Arbeitsgruppen eingerichtet oder aus der Projektphase fortgesetzt (z.B. Arbeitsgruppe Portal / Metadaten).

Nr. 40: Bund, Kantone und Gemeinden fördern offene und partizipative Systeme und Prozesse (z.B. Open Data, Open Access, Open Science, Open Innovation, Citizen Science, Hackathons, Fablabs, Makerspaces, Gov Labs und City Challeges), um gesellschaftliche Ziele wie digitale Transformation, Resilienz und Nachhaltigkeit schneller zu erreichen.

Zuständig: EFD, UVEK, EDA

Rückmeldung: EFD: Annahme
Rückmeldung UVEK: Annahme
Rückmeldung EDA: Annahme

EFD: Die Arbeiten sind zu koordinieren mit E-Gov Schweiz.

UVEK: Diese Arbeiten laufen z.T. bereits im Rahmen der Strategie Digitale Schweiz.[9]

EDA: Siehe hierzu auch das EDA-Projekt «Weiterentwicklung der Demokratie auf Basis einer digitalen Selbstbestimmung»[10].

Nr. 42: Bund und Kantone stellen sicher, dass Blockchain-Lösungen bei sensitiven Anwendungen in der Verwaltung und in regulierten Bereichen nur dann zur Anwendung kommen, wenn eine langfristige Sicherheit (z.B. rechtzeitige Aktualisierungen) gewährleistet ist.

Zuständig: EFD

Rückmeldung EFD: Annahme

EFD: Die betroffenen Regulatoren müssten ebenfalls einbezogen werden.

Nr. 43: Der Bund nimmt, unter Berücksichtigung der regulatorischen Entwicklungen im Ausland, die nötigen rechtlichen Anpassungen bei der Behandlung von digitalen „Datenpaketen“ (Tokens), von digital geführten Registern und im Bereich des Datenschutzes vor.

Zuständig: EJPD

Rückmeldung EJPD: teilweise Annahme

[9] https://strategy.digitaldialog.swiss/aktionsplan

[10] https://strategy.digitaldialog.swiss/de/aktionsplan/4

EJPD: Der Bundesrat hat am 7. Dezember 2018 einen Bericht zu den rechtlichen Rahmenbedingungen für Blockchain und Distributed-Ledger-Technologie im Finanzsektor verabschiedet.[11] Die Analysen zeigen, dass sich keine grundlegenden Anpassungen des Schweizer Rechtsrahmens aufdrängen, aber dennoch punktueller Anpassungsbedarf besteht. Der Bundesrat hat das EFD und das EJPD beauftragt, im 1. Quartal 2019 eine Vernehmlassungsvorlage zu erarbeiten, unter anderem mit dem Ziel, im Zivilrecht die Rechtssicherheit bei der Übertragung von Rechten mittels digitalen Registern zu erhöhen und im Insolvenzrecht die Aussonderung im Konkurs von kryptobasierten Vermögenswerten weiter zu klären sowie eine Aussonderung von nicht vermögenswerten Daten zu prüfen.

Nr. 44: Bund und Kantone sorgen dafür, dass die Schülerinnen und Schüler im Rahmen der obligatorischen Schule und alle Studierenden die notwendigen Grundfertigkeiten und Kompetenzen für den Umgang und die Gestaltung mit digitalen Technologien und der Transformation entwickeln.

Zuständig : Zuständigkeit obligatorische Schule: Kantone; Zuständigkeit Hochschulen: Hochschulen, Kantone und Bund

Rückmeldung WBF: Annahme

WBF: Bund und Kantone sind in diesem Bereich bereits sehr aktiv. Im Bericht «Herausforderungen der Digitalisierung für Bildung und Forschung in der Schweiz»[12] wird mehrmals betont, dass das Schweizer Bildungssystem an die digitalen Entwicklungen angepasst werden muss. Zu diesem Zweck werden im Aktionsplan verschiedene Massnahmen vorgeschlagen, um in Zusammenarbeit mit den Kantonen den Erwerb digitaler Kompetenzen auf allen Bildungsebenen zu verbessern und zu stärken. Einige dieser Massnahmen wurden bereits umgesetzt, andere laufen. Im Hochschulbereich wird die Vermittlung von digitalen Anwendungskompetenzen über die projektgebundenen Beiträge in den Jahren 2019–2020 gefördert.

Es sei darauf hingewiesen, dass die EDK mit der Verabschiedung ihrer «Strategie für den Umgang mit Wandel durch Digitalisierung im Bildungswesen»[13] vom 21. Juni 2018 ebenfalls die Bedeutung von Massnahmen in diesem Bereich erkannt hat. Schliesslich stellen Bund und Kantone im Rahmen des Koordinationsausschusses Digitalisierung in der Bildung (KoA Digi) die Koordination und Kohärenz ihrer jeweiligen Strategien sicher.

Nr. 46: Bund und Kantone setzen sich für eine Kulturförderung ein, die sich verstärkt mit dem digitalen Wandel auseinandersetzt, und schaffen öffentliche Räume für den kreativen Umgang mit digitalen Technologien.

Zuständig: EDI

Rückmeldung EDI: Teilweise Annahme

EDI: Die Empfehlung richtet sich an Bund und Kantone. In Bezug auf den Bund wird die Empfehlung angenommen. Der Bundesrat hat in der Vernehmlassungsvorlage vom 29. Mai 2019 der Botschaft zur Förderung der Kultur in den Jahren 2021-2024 (Kulturbotschaft)[14] festgehalten, dass er in den nächs-

[11] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73398.html
[12] https://www.sbfi.admin.ch/sbfi/de/home/das-sbfi/digitalisierung.html
[13] http://www.edk.ch/dyn/31425.php
[14] Vernehmlassungsunterlagen zur Kulturbotschaft 2021–2024

ten Jahren einen Schwerpunkt auf Massnahmen legen will, die sich für die Kultur aus den Herausforderungen der Digitalisierung ergeben. Keinen direkten Einfluss hat der Bund dagegen auf die Kulturpolitik der Kantone.

Nr. 47: Bund und Kantone setzen sich dafür ein, dass der Schutz von Grundwerten, Menschenrechten und Menschenwürde auch im digitalen Zeitalter gesichert und die informationelle Selbstbestimmung gefördert werden.

Zuständig: EJPD, EDA

Rückmeldung EJPD: Annahme

Rückmeldung EDA: Annahme

EJPD: Diese Empfehlung betrifft eine Daueraufgabe, welche das BJ bereits wahrnimmt. Das BJ ist derzeit mit mehreren Geschäften befasst, welche dieser Empfehlung Rechnung tragen. Zu nennen ist insbesondere die Totalrevision des DSG. Auch mit der geplanten Ratifizierung der modernisierten Datenschutz-Konvention SEV 108 des Europarates soll die informationelle Selbstbestimmung gestärkt werden. Weiter zu erwähnen ist die Teilnahme des BJ in der bundesverwaltungsinternen Arbeitsgruppe zum Thema der «Künstlichen Intelligenz».

EDA: Von besonderem Interesse für das EDA ist die Frage, ob private Akteure im Bereich Anwendungen und Cybersicherheit das humanitäre Völkerrecht und die Menschenrechte beachten. Es bleibt abzuwarten, inwieweit dieser spezifische Aspekt in diesem allgemeineren Rahmen berücksichtigt werden kann.

Nr. 50: Der Bund sorgt für ausreichende Transparenz, Nachvollziehbarkeit, Verständlichkeit und Accountability (Rechenschaftspflicht) bei digitalen Prozessen und Algorithmen, um eine vertrauensbasierte digitale Wirtschaft und Gesellschaft zu gewährleisten.

Zuständig: WBF

Rückmeldung WBF: Das Thema wird im Zusammenhang mit dem Auftrag des Bundesrates an das WBF zur Künstlichen Intelligenz bearbeitet (Interdepartementale Arbeitsgruppe Künstliche Intelligenz, IDAG KI). Ein entsprechender Bericht soll im 2. Semester 2019 vorliegen.[15]

3.2 Abgelehnte Empfehlungen der Expertengruppe

Folgende Empfehlungen sollen zum gegenwärtigen Zeitpunkt nicht explizit weiterverfolgt werden:

Nr. 1: Der Bund setzt sich dafür ein,

- **dass die Eidgenössischen Technischen Hochschulen, die Universitäten sowie die Fachhochschulen und Berufsbildungsinstitutionen mit Ausbildungsangeboten im Bereich der IKT die Informationssicherheit ausbauen und vernetzen und die dafür minimal notwendigen Lerninhalte festlegen;**

[15] https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/medienmitteilungen.msg-id-72053.html

- **dass die Informationssicherheit bei den Eidgenössischen Technischen Hochschulen, den Universitäten sowie den Fachhochschulen und Berufsbildungsinstitutionen Teil der Grundausbildung wird.**

Zuständig: WBF, ETH-Rat, Mitinteresse VBS

Rückmeldung des WBF/SBFI: Ablehnung
Rückmeldung des VBS: Ablehnung

WBF: Aus Sicht des SBFI, und in Übereinstimmung mit dem Generalsekretariat der Rektorenkonferenz schweizerischen Hochschulen (swissuniversities), ist die erste Empfehlung in dieser Form abzulehnen. Die Schaffung sowie die Gestaltung von Aus- und Weiterbildungsangeboten im Hochschulbereich fällt in die Autonomie der Hochschulen. Weder der Bund noch die Kantone können den Hochschulen Ausbildungsangebote oder Lerninhalte vorschreiben. Das SBFI wird den Expertenbericht sowie die Empfehlungen betreffend die Hochschulen swissuniversities zur Kenntnis bringen. Im Bericht «Herausforderungen der Digitalisierung für Bildung und Forschung in der Schweiz» hat der Bundesrat Handlungsbedarf im Bereich der Vermittlung von Anwendungskompetenzen digitaler Technologien («Digital Skills») in allen Fachbereichen identifiziert. Die Hochschulen werden in den Jahren 2019-2020 unter anderem auch Kooperationsprojekte hinsichtlich der sich wandelnden curricularen Anforderungen umsetzen. Die Schweizerische Hochschulkonferenz SHK hat swissuniversities ausserdem bereits beauftragt, das Thema Digitalisierung schwerpunktmässig in die strategische Planung der Hochschulen für die Jahre 2021-2024 aufzunehmen.

In der beruflichen Grundbildung vermittelt der allgemein bildende Unterricht (ABU) grundlegende Kompetenzen. Die Verantwortung für den entsprechenden Rahmenlehrplan liegt beim Bund, für die konkrete Umsetzung sind jedoch die Kantone verantwortlich. Die Empfehlung ist auch aus Sicht der beruflichen Grundbildung abzulehnen, weil im Rahmen des Strategieprozesses «Berufsbildung 2030» auch der Rahmenlehrplan ABU angegangen und als Projekt «ABU 2030» überarbeitet wird. Die notwendigen Schritte wurden somit bereits in die Wege geleitet und stützen sich auf den Auftrag aus dem «Aktionsplan Digitalisierung im BFI-Bereich in den Jahren 2019 und 2020».

VBS: Das VBS schliesst sich den Erläuterungen des WBF an. Es weist zudem darauf hin, dass auch in der Armee zahlreiche Aktivitäten im Hinblick auf eine Ausbildung im Cyber-Bereich stattfinden, z.B. der Aufbau des Cybercampus und der neu geschaffene Cyberlehrgang (s. auch Bemerkung zu Empfehlung 7).

Nr. 9: Der Bund prüft, ob die geltenden Strafnormen ausreichen, um bei der Verletzung von Geheimnissen durch digitale Systeme (z.B. durch personalisierte Applikationen) den Verursacher zur Verantwortung ziehen zu können.

Zuständig: EJPD, VBS; Mitinteresse EDA

Rückmeldung EJPD: Ablehnung
Rückmeldung VBS: Ablehnung
Rückmeldung EDA: Mitinteresse

EJPD: Die strafrechtlichen Regeln zum Geheimnisschutz sind ausreichend:

Wer als Geheimnisherr oder als Geheimnisträger IKT-Mittel einsetzt, ist verpflichtet, die Risiken eines solchen Einsatzes zu prüfen und gegebenenfalls geeignete Massnahmen zu treffen (Einwilligungen einholen, Verschlüsselungen einsetzen, NDA abschliessen, auf den Einsatz verzichten und Alternativen prüfen etc.). Geht ein aufgeklärter Geheimnisherr solche Risiken trotzdem ein, ist darin eine (konkludente) strafrechtliche Einwilligung zu sehen. Die Konsequenzen von Geheimnisoffenbarungen liegen danach nicht mehr im strafrechtlichen Bereich. Geht ein aufgeklärter Geheimnisträger solche Risiken ein, ohne die erforderlichen Massnahmen (insb. Einwilligungen einholen oder Verschlüsselungen

einsetzen) zu treffen, macht er sich grundsätzlich strafbar. Die fahrlässige Geheimnisverletzung ist nach geltendem Recht nicht strafbar. Sie scheint im vorliegenden Zusammenhang auch kaum relevant: Wer IKT-Mittel jedenfalls beruflich einsetzt oder einsetzen lässt, weiss, dass die fraglichen Daten («Geheimnisse») oft bei Dritten (u.U. auch im Ausland) gespeichert werden. Darauf zu vertrauen, dass Dritte strafrechtlich geschützte Informationen nicht wahrnehmen, ist nicht relevant: Bei der Tathandlung «Offenbaren» reicht die Möglichkeit der Kenntnisnahme von unberechtigten Personen aus, weshalb hier regelmässig Eventualvorsatz gegeben ist.

Dass jemand «Verursacher» (so die Formulierung der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit») einer Geheimnisverletzung ist, reicht aus rechtsstaatlichen Gründen (Schuldprinzip) weder für eine Bestrafung von Personen noch von Unternehmen aus: Es wäre verfehlt, die Hersteller und Betreiber von IKT-Systemen für Geheimnisverletzungen zu bestrafen, von denen sie keine Kenntnis haben (können). Kausalhaftungen sind dem schweizerischen Strafrecht fremd. Hersteller und Betreiber von IKT-Systemen sind aber ggf. als Hilfspersonen des Geheimnisträgers oder des Geheimnisherrn nach Massgabe von Artikel 162 StGB (für Geschäftsgeheimnisträger) oder Artikel 321 StGB (für Berufsgeheimnisträger) strafbar. Gemäss dem Entwurf des Bundesrates zur Revision von Artikel 320 StGB soll diese Strafbarkeit von Hilfspersonen auch beim Schutz von Amtsgeheimnissen – insbesondere im IKT-Bereich – gelten (siehe dazu den Entwurf zu Art. 320 E-StGB im Geschäft 17.028 Informationssicherheitsgesetz). Die Sachlage weist Parallelen auf zur Strafbarkeit von Hosting-Providern wegen Gehilfenschaft zu Straftaten ihrer Nutzer.

Wegen der über Landesgrenzen hinweg agierenden IKT-Dienstleister ergeben sich oft Probleme bei der Rechtsdurchsetzung: Für Strafbehörden ist es aus völkerrechtlichen (Souveränitäts- und Territorialitätsprinzip) und aus praktischen Gründen (insb. wegen des sog. «loss of knowledge of location») schwierig, Unternehmensangehörigen eine strafrechtliche Verantwortlichkeit für Geheimnisverletzungen nachzuweisen, die durch den Betrieb von IKT-Systemen entstehen können. Durch vertragliche und technische Vorkehrungen des Auftraggebers lassen sich praktische Schwierigkeiten jedoch zumindest teilweise ausräumen. Der Bundesrat wird dem Parlament im Rahmen der Umsetzung der Mo. 18.3379 RK-S (Zugriff der Strafverfolgungsbehörden auf Daten im Ausland) eine Regelung vorschlagen, damit die Rechtsdurchsetzung bei grenzüberschreitenden Sachverhalten verbessert werden kann; er wirkt auch auf internationaler Ebene auf dieses Ziel hin.

VBS: Das VBS ist mit der Stellungnahme des EJPD grundsätzlich einverstanden. Allenfalls sind jeweils Schnittstellen zur Militärpolizei (Armee) und zur Militärjustiz (Oberauditor GS VBS) zu berücksichtigen.

EDA: Es besteht ein Mitinteresse wegen möglichem internationalen Bezug.

Nr. 13: Der Bund setzt sich in Zusammenarbeit mit der Wirtschaft für die Einführung von Instrumenten ein, die zum Ziel haben, im Zusammenhang mit Online-AGB einen angemessenen Konsumentenschutz zu gewährleisten.

Zuständig: EJPD, WBF

Rückmeldung EJPD: Ablehnung
Rückmeldung WBF: Ablehnung

EJPD: Der Einbezug und die Kontrolle von AGB in Verträge mit Konsumentinnen und Konsumenten wird durch die vom Bundesgericht entwickelten Regeln sowie durch den am 1. Juli 2012 in Kraft getretenen Artikel 8 UWG festgelegt (Inhaltskontrolle). Auch wenn es kaum Gerichtsentscheide zu Artikel 8 UWG gibt, hat diese Bestimmung eine Ausstrahlung auf die Vertragspraxis. Es handelt sich nicht um ein besonderes Problem des Online-Handels, und es ist nicht ersichtlich, weshalb dort spezielle Regeln gelten sollen. Die geltende Regelung ist ausreichend. Zudem handelt es sich um einen hochpolitischen Entscheid; jede Anpassung bedarf eines klaren Auftrags des Parlaments.

WBF: Dem SECO fehlt eine gesetzliche Grundlage, um sich in Zusammenarbeit mit der Wirtschaft für die Einführung von Instrumenten einzusetzen, die zum Ziel haben, im Zusammenhang mit Online-AGB einen angemessenen Konsumentenschutz zu gewährleisten.

Generell kann der Bund, vertreten durch das SECO, gestützt auf Art. 10 Abs. 3 UWG (Bundesgesetz gegen den unlauteren Wettbewerb; SR 241), wenn er es zum Schutz des öffentlichen Interesses als nötig erachtet, lediglich mittels Zivilklage und in den von Art. 23 Abs. 1 UWG umfassten Fällen mittels Strafantrag gegen Personen oder Unternehmen vorgehen, die durch unlautere Geschäftspraktiken entweder das Ansehen der Schweiz im Ausland oder Kollektivinteressen im Inland bedrohen oder verletzen. Das SECO nimmt dieses Klagerecht grundsätzlich nur wahr, wenn es entsprechende Beschwerden erhält, die eine Gefährdung bzw. Verletzung öffentlicher Interessen darlegen. Demgegenüber stellt Art. 10 Abs. 3 UWG keine gesetzliche Grundlage dar, die den Bund bzw. das SECO ermächtigen würde, in Zusammenarbeit mit der Wirtschaft «Instrumente» einzuführen, die zum Ziel haben, im Zusammenhang mit Online-AGB einen angemessenen Konsumentenschutz zu gewährleisten.

Zudem ist zu bedenken, dass der Schutzbereich von Art. 8 UWG auf eigentliche Missbrauchsfälle beschränkt ist und lediglich festlegt, wann allgemeine Geschäftsbedingungen (AGB) missbräuchlich sind. Das SECO hat nur die Möglichkeit, Verwender von im Sinne von Art. 8 UWG missbräuchlichen AGB abzumahnen und nötigenfalls auf dem Zivilprozessweg gegen sie vorzugehen, wenn die Voraussetzungen von Art. 10 Abs. 3 UWG gegeben sind.

Nr. 14: Der Bund prüft die Frage, ob ein angemessenes Widerrufsrecht bei Online-Geschäften einzuführen ist.

Zuständig: EJPD

Rückmeldung EJPD: Ablehnung

EJPD: Das Parlament hat es im Rahmen der Behandlung der Pa.Iv. 06.441[16] im Jahr 2013 bewusst abgelehnt, ein Widerrufsrecht für Fernabsatzverträge nach dem Vorbild des europäischen Rechts zu übernehmen. Seither hat es keine Veränderungen gegeben, die ein Zurückkommen auf diesen Entscheid nahelegen würden. Zudem handelt es sich um einen hochpolitischen Entscheid; jede Anpassung bedarf eines klaren Auftrags des Parlaments.

Nr. 16: Der Bund prüft, ob mittelfristig sektorspezifische Regulierungen, z.B. im Wettbewerbsrecht (UWG), in der Preisbekanntgabeverordnung oder im Versicherungsrecht nötig sind.

Zuständig: WBF

Rückmeldung WBF: Ablehnung

WBF: Die Preisbekanntgabeverordnung (PBV) bezweckt, dass Preise klar und miteinander vergleichbar sind und irreführende Preisangaben verhindert werden. Auch bei dynamischen Preisen ist die PBV anwendbar und es müssen insbesondere die tatsächlich zu bezahlenden Preise bekanntgegeben sowie spezifiziert werden. Werden die Vorschriften der PBV eingehalten, haben Preisdifferenzierungen aufgrund von Datenanalysen deshalb keine negativen Auswirkungen auf die Klarheit und Vergleichbarkeit von Preisen sowie die Verhinderung irreführender Preise. Einzig extrem kurze Gültigkeitsdauern dynamischer Preise könnten in Konflikt mit dem Zweck der PBV stehen. Die Festlegung einer Mindestgültigkeitsdauer von Preisen ist derzeit jedoch nicht angebracht. Dynamische Preise sind aktuell ausreichend lange gültig, um eine Vergleichbarkeit der Preise sicherzustellen und eine zeitliche

[16] 06.441 Parlamentarische Initiative Mehr Konsumentenschutz und weniger Missbräuche beim Telefonverkauf, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20060441

Regulierung könnte stattdessen die allgemeine Verkürzung der Preisgültigkeitsdauern zur Folge haben. Zudem steht die Gültigkeitsdauer von Preisen nicht in direktem Zusammenhang mit der Problematik der Preisdifferenzierung aufgrund von Datenanalysen. Eine flächendeckende Regulierung in der PBV ist nicht nötig. Allfällige sektorspezifische Regulierungen wären in den Spezialgesetzen und nicht in der PBV zu prüfen.

Nr. 17: Der Bund fördert Online-Beschwerde- und -Streitschlichtungsmechanismen (Online Dispute Resolution, ODR), unter Einbezug privater Angebote.

Zuständig: EJPD, WBF

Rückmeldung EJPD/BJ: Ablehnung
Rückmeldung WBF: Ablehnung

EJPD und WBF: Online-Beschwerde und Streitschlichtungsmechanismen (ODR) sind anerkanntermassen effiziente und erfolgreiche Instrumente zur aussergerichtlichen Streitbeilegung, welche den justizförmigen Rechtsschutz sinnvoll ergänzen. Als Beispiel einer gesetzlich vorgesehenen Schlichtungsstelle kann etwa die Ombudscom im Bereich der Telekommunikation genannt werden (https://de.ombudscom.ch/gesetzliche-grundlagen/). Die Ombudscom ist eine Stiftung und insoweit nicht Teil der Bundesverwaltung, wenn sie auch unter der Aufsicht des BAKOM steht. Die Bundesverwaltung beobachtet den Einsatz dieser Mechanismen laufend und wird bei Bedarf darüber befinden, ob Fördermassnahmen in diesem Bereich vonnöten sind und auf welcher gesetzlichen Grundlage diese basieren sollen.

Nr. 18: Der Bund prüft im Kartellrecht, ob nicht alternativ zu den Umsatzschwellenwerten auch die Transaktionswerte geeignete Aufgreifkriterien bei der Prüfung von Unternehmenszusammenschlüssen wären.

Zuständig: WBF

Rückmeldung WBF: Ablehnung

WBF: Der Bundesrat hat das Thema bereits in seinem «Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft» von 2017[17] diskutiert. Eine vom SECO in Auftrag gegebene Studie[18] hat diese Frage beleuchtet. Darin wird in eine Reform der Aufgreifkriterien zum heutigen Zeitpunkt von den befragten Experten mit einer Ausnahme abgelehnt sowie als übereilt bezeichnet. Vor dem beschriebenen Hintergrund sieht das SECO derzeit keinen weiteren Handlungsbedarf.

Nr. 19: Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, ob das Risiko einer durch Preisalgorithmen verursachten Kollusion im Kartellgesetz präziser geregelt werden soll.

Zuständig: WBF

Rückmeldung WBF: Ablehnung

WBF: Das geltende Kartellgesetz erfasst grundsätzlich auch Sachverhalte betreffend die Abstimmung mittels Preisalgorithmen. Einen Änderungsbedarf der gesetzlichen Regelungen besteht zurzeit nicht.

---

[17] https://www.seco.admin.ch/seco/de/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html#2070061810
[18] https://www.seco.admin.ch/seco/de/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/Wettbewerbspolitik/kartellgesetz/revision-fusionskontrolle.html

Die Ausführungen zu den Überlegungen der Bundesverwaltung hinsichtlich Preisalgorithmen (S.100 vierter Absatz) sind zudem unzutreffend. Sowohl das SECO als auch die Wettbewerbsbehörden haben sich hierzu durchaus bereits ausführliche Gedanken gemacht (u.a. auch im Rahmen diverser Fachtagungen).

Nr. 22: Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen eine Regelung der Portabilität von Sachdaten.

Zuständig: EJPD

Rückmeldung EJPD: Ablehnung

EJPD: Die Frage des Zugangs zu nicht-personenbezogenen Daten wird im Rahmen der Empfehlung 20 (siehe oben) recht umfassend untersucht. Daher ist es zum jetzigen Zeitpunkt nicht angebracht, parallel Arbeiten zur Portabilität von nicht-personenbezogenen Daten durchzuführen. Darüber hinaus enthält der Expertenbericht nur sehr wenige Elemente zur Unterstützung dieser Empfehlung. Die darin angedeuteten internationalen Entwicklungen gehen nicht so weit, dass Rechte oder Pflichten eingeführt werden: Die EU-Verordnung 2018/1807 vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU sieht lediglich vor, dass die Europäische Kommission mittels Selbstregulierung die Entwicklung von Verhaltensregeln fördert und erleichtert, um die Datenübertragung zu erleichtern. Da die EU eine Selbstregulierung bevorzugt, erscheint es zum jetzigen Zeitpunkt nicht sinnvoll, den Regelungsbedarf im Schweizer Recht zu prüfen. Schliesslich stellt sich die Frage, ob es nicht zweckmässiger wäre, wenn die Departemente den Regelungsbedarf sektorspezifisch in ihren jeweiligen Zuständigkeitsbereichen (Energie, Fahrzeuge usw.) unter Berücksichtigung der dazugehörigen Besonderheiten untersuchten, anstatt allgemeine Bestimmungen einzuführen. Wir schlagen daher vor, diese Empfehlung vorerst nicht weiter zu prüfen, um sich voraussichtlich unnötige Arbeit zu ersparen, zumal die in der EU-Verordnung vorgesehenen Verhaltensregeln auf internationaler Ebene wohl erst am Anfang stehen. Ausserdem sollte das Ergebnis der Arbeiten zur Empfehlung 20 abgewartet werden.

Nr. 23: Der Bund schliesst Lücken betreffend die Rechte der Betroffenen beim Rechtsschutz, insbesondere durch Anpassungen des Bundesgesetzes über Schuldbetreibung und Konkurs und des Erbrechts.

Zuständig: EJPD:

Rückmeldung EJPD: Ablehnung

EJPD: Die entsprechenden Arbeiten sind bereits am Laufen. Im SchKG wird eine besondere Bestimmung zur Aussonderung von Daten im Rahmen der Blockchain-Vorlage in die Vernehmlassung geschickt. Im Erbrecht wird die betreffende Problematik im Rahmen des Postulats 14.3782 [19]behandelt. Der Empfehlung wird ausserdem im Rahmen der Totalrevision des DSG durch Art. 16 E-DSG teilweise Rechnung getragen. Diese Bestimmung regelt, unter welchen Bedingungen Einsicht in die Personendaten einer verstorbenen Person gewährt wird und unter welchen Voraussetzungen die Erben oder der Willensvollstrecker die Löschung bzw. Vernichtung der Personendaten einer verstorbenen Person verlangen können.

[19] Postulat 14.3782 Schwaab Jean Christophe vom 24.09.2014 Richtlinien für den «digitalen Tod», https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143782

Nr. 24: Der Bund prüft unter Berücksichtigung der internationalen Entwicklungen, insbesondere derjenigen in der EU, den Handlungsbedarf im ausservertraglichen Haftungsrecht (Produktehaftung, Produktesicherheit, Providerhaftung, Netzwerkinfrastrukturhaftung) und die allfällige Einführung neuer Haftungskonzepte.

Zuständig: EJPD

Rückmeldung EJPD: Ablehnung

EJPD: Zurzeit ist kein Handlungsbedarf ersichtlich. Die betreffenden Fragen wurden teilweise auch bereits geprüft. Soweit sich in der Praxis Probleme stellen, werden diese spezifisch angegangen, generelle Lösungen erscheinen hier wenig sinnvoll.

Hinsichtlich der von der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» genannten «Netzwerkinfrastrukturhaftung» und der erneut zur Diskussion gestellten Providerhaftung und ist auf die Arbeiten des Bundesrates und des Parlaments zur Bekämpfung von Netzwerkkriminalität und den Bericht des Bundesrates zur zivilrechtlichen Providerhaftung[20] zu verweisen: Danach sind neuartige Haftungskonzepte in diesem Bereich nicht notwendig und bieten keine Vorteile gegenüber der heute geltenden Regeln. Es ist nicht ersichtlich, inwiefern die Erkenntnisse der Expertengruppe etwas an diesem Befund geändert hätten. Punktuelle strafrechtliche Anpassungen in den Gesetzen zur Produktesicherheit oder zur Produktehaftung sind akzessorisch bei einer allfälligen Revision dieser Gesetze zu prüfen.

Nr. 30: Der Bund prüft,

- **ob Betreiber kritischer Infrastrukturen eine Betriebssicherheitserklärung vorweisen müssen;**
- **ob und wie das Betriebssicherheitsverfahren auch Stellen ausserhalb des Bundes und der Verwaltung bei sensitiven Beschaffungen zur Verfügung gestellt werden kann.**

Zuständig: VBS

Rückmeldung VBS: Ablehnung

VBS: Es zählen auch Betriebe zu den kritischen Infrastrukturen, welche vorwiegend als Zulieferer von Bedeutung sind. Nicht alle KI-Betreiber können über einen Kamm geschert werden. Wir sehen durch ein solches Vorgehen ausserhalb von einzelnen spezifischen Bereichen und Spezial-Gesetzgebungen keinen grossen Mehrwert und ein schlechtes Kosten-Nutzen-Verhältnis. Dies gilt für Prüfer und Geprüfte.

Nr. 34: Der Bund prüft zusammen mit den Kantonen eine Harmonisierung des öffentlich-rechtlichen Datenschutzes in der Schweiz.

Zuständig: EJPD

Rückmeldung EJPD: Ablehnung

EJPD: Wie im Bericht der Expertengruppe zur «Zukunft der Datenbearbeitung und Datensicherheit» erläutert (S. 133), wurde die Frage, ob die geltende Kompetenzverteilung zwischen Bund und Kantonen im Bereich des Datenschutzes noch adäquat ist oder ob eine Harmonisierung angestrebt werden soll, bereits im Rahmen der Arbeiten zur Totalrevision des DSG geprüft. Eine von der Konferenz der Kantonsregierungen im Herbst 2013 durchgeführte Anhörung hat ergeben, dass eine klare Mehrheit

[20] https://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-d.pdf

der Kantone eine Kompetenz des Bundes, die allgemeine Datenschutzgesetzgebung zu vereinheitlichen, ablehnt. Bei der Totalrevision des DSG wurde deshalb auf eine Anpassung der Kompetenzverteilung zwischen Bund und Kantonen und auf die dafür nötige vorgängige Verfassungsrevision verzichtet. Nach unserer Einschätzung hat sich diese Ausgangslage in der Zwischenzeit nicht verändert. Hinzu kommt, dass aktuell nicht nur der Bund, sondern auch die Kantone eine Revision ihrer Datenschutzgesetzgebungen durchführen, um den neuen europäischen Datenschutzstandards Rechnung zu tragen. Dies dürfte zu einer weiteren inhaltlichen Annäherung führen. Vor diesem Hintergrund sind wir der Ansicht, dass Überlegungen zur Harmonisierung des öffentlichen Datenschutzrechts zum jetzigen Zeitpunkt nicht zweckmässig sind.

Nr. 41: Bund und Kantone dehnen E-Voting-Projekte nur aus, wenn aufgezeigt werden kann, dass E-Voting nicht mit grösseren Risiken verbunden ist als die bestehenden Formen der demokratischen Mitwirkung bei Wahlen und Abstimmungen. Wahl- und Abstimmungsergebnisse müssen überprüfbar bleiben.

Zuständig: BK, Mitinteresse EDA

Rückmeldung BK: Ablehnung
Rückmeldung EDA: Mitinteresse

BK: Die Empfehlung würde eine Vergleichbarkeit mit den Risiken von «bestehenden Formen der demokratischen Mitwirkung», also der brieflichen und der persönlichen Stimmabgabe an der Urne, bedingen. Dieser Teil der Empfehlung ist nicht umsetzbar, da die Kriterien zum Vergleich der Risiken unklar sind und die Risiken von «bestehenden Formen der demokratischen Mitwirkung» nicht in quantifizierter Form bekannt sind. Es muss weiterhin das Ziel sein, die spezifischen Risiken aller Stimmkanäle so tief als möglich zu halten. So berücksichtigen die bundesrechtlichen Anforderungen (insbesondere Verifizierbarkeit, Zertifizierung, Transparenz) für den Einsatz der elektronischen Stimmabgabe die spezifischen Risiken dieses Stimmkanals. Es werden nur E-Voting-Systeme zugelassen, welche die hohen bundesrechtlichen Sicherheitsanforderungen erfüllen. Artikel 3 der VEleS (Verordnung der BK vom 13. Dezember 2013 über die elektronische Stimmabgabe; SR 161.116) fordert im Rahmen der für den Einsatz von E-Voting nötigen Grundbewilligung und Zulassung die laufende Risikobeurteilung. Allfällige mit einem breiteren Einsatz der elektronischen Stimmabgabe verbundene Risiken werden ebenfalls im Rahmen dieser Prozesse beurteilt. Nur wenn sich jegliche Sicherheitsrisiken in ausreichend tiefem Rahmen bewegen, darf die elektronische Stimmabgabe eingesetzt werden. Die Verifizierbarkeit (Art. 4 und 5 VEleS) bietet gestützt auf spezielle kryptografische Verfahren Transparenz über den korrekten Ablauf des Urnengangs, dies unter Wahrung des Stimmgeheimnisses. Damit ist das E-Voting überprüfbar konzipiert (zweiter Teil der Empfehlung) und lässt sich besonders wirksam vor unbemerkten Manipulationen schützen. Im Übrigen hat die Vernehmlassung zur Änderung des Bundesgesetzes über die politischen Rechte (BPR; SR 161.1) zur Verankerung der elektronischen Stimmabgabe als dritter ordentlicher Stimmkanal gezeigt, dass eine deutliche Mehrheit der Kantone und der Parteien die Einführung von E-Voting grundsätzlich begrüsst, der Zeitpunkt zur Überführung in den ordentlichen Betrieb aber als verfrüht angesehen wird. Daher hat der Bundesrat an seiner Sitzung vom 26. Juni 2019 beschlossen, vorerst auf die Teilrevision des BPR zu verzichten und die Bundeskanzlei beauftragt, mit den Kantonen bis Ende 2020 eine Neuausrichtung des Versuchsbetriebs sicherzustellen.

DA: e-Voting a une grande importance aussi pour les Suisses de l’étranger.

EDA: E-Voting ist auch für die Auslandschweizerinnen und Auslandschweizer von grosser Bedeutung. Dieser Aspekt sollte bei den Überlegungen Beachtung finden.

Nr. 45: Bund und Kantone schaffen in enger Zusammenarbeit mit allen betroffenen Kreisen der Gesellschaft und Wirtschaft die strukturellen Voraussetzungen, um die Weiterbildung für Berufsleute aller Bereiche zwecks Bewältigung der digitalen Transformation zu erleichtern.

Zuständig: WBF

Rückmeldung WBF: Ablehnung

WBF: Das SBFI beantragt die Ablehnung dieser Empfehlung. Mit Berufsbildungsgesetz und Weiterbildungsgesetz hat der Bund schon jetzt die strukturellen Voraussetzungen und Zuständigkeiten definiert, die für Berufsbildung und Weiterbildung gelten. Für die Definition der Inhalte einer Berufs- oder Weiterbildung sind die betroffenen Kreise der Wirtschaft selbst verantwortlich. Besonders hervorzuheben gilt es in Zusammenhang mit den vorgeschlagenen Massnahmen bzw. Fragestellungen in Kapitel 10.3.3 auch Artikel 5 des Weiterbildungsgesetzes.

Nr. 48: Bund und Kantone sorgen in Zusammenarbeit mit den verantwortlichen Behörden und Anbietern im Bereich der Berufsausbildung dafür, dass die Ethik zu einem festen Bestandteil der Aus- und Weiterbildung wird, und nehmen diese Aspekte in ihre Erwartungen an das verantwortungsvolle Unternehmertum auf.

Zuständig: WBF

Rückmeldung WBF Ablehnung

WBF: Das SBFI lehnt die Empfehlung ab, da sie bereits erfüllt ist. Die Verantwortung für den entsprechenden Rahmenlehrplan liegt beim Bund, für die konkrete Umsetzung sind jedoch die Kantone verantwortlich. Der Aspekt Ethik ist im Lernbereich Gesellschaft bereits Teil des Rahmenlehrplans. Im Bereich der Weiterbildung liegen die Zuständigkeiten für die Inhalte nicht beim Bund.

Nr. 49: Bund und Kantone schaffen die Voraussetzungen dafür, dass Hochschulen und Weiterbildungseinrichtungen Forschung und Lehre in den Bereichen „Responsible Innovation“ (verantwortungsvolle Innovation) und „Design for Values“ (Werte-orientiertes Design) intensivieren.

Zuständig WBF, ETH-Rat

Rückmeldung WBF: Ablehnung

WBF: Das SBFI, in Übereinstimmung mit dem Generalsekretariat von swissuniversities, lehnt die Empfehlung ab. Die Gestaltung von Aus- und Weiterbildungsangeboten sowie der Lehr- und Lernformen im Hochschulbereich fällt in die Autonomie der Hochschulen. Das SBFI wird den Expertenbericht sowie die Empfehlungen betreffend die Hochschulen swissuniversities zur Kenntnis bringen.

Nr. 51: Der Bund schafft die nötigen rechtlichen Grundlagen, um sicherzustellen, dass bei elektronischer interaktiver Kommunikation transparent gemacht wird, wenn die Kommunikation nicht mit einem Menschen erfolgt.

Zuständig: WBF, UVEK

Rückmeldung WBF: Ablehnung
Rückmeldung UVEK: Ablehnung

WBF und UVEK: Es ist unklar, inwiefern das in der Empfehlung beschriebene «Problem» in der Praxis heute tatsächlich besteht. Erstens ist die Verbreitung solch «maschineller» Kommunikation nicht

bekannt, zweitens ist nicht klar, ob «maschinelle» Kommunikation nicht freiwillig transparent gemacht wird. Solange keine gesicherten Erkenntnisse dazu vorliegen sollte keine «Regulierung auf Vorrat» eingeführt werden.

3.3 Laufende Aktivitäten, Annahme oder Ablehnung möglich

Nr. 39: Bund, Kantone und Gemeinden treffen geeignete Massnahmen, um Pilotprojekte mit innovativen Ansätzen der partizipativen Demokratie wie „Massive Open Online Deliberation“ zu fördern und Grundlagen für deren Beurteilung zu schaffen.

Zuständig: BK, Mitinteresse EDA

Rückmeldung BK: Annahme oder Ablehnung, abhängig von laufenden Arbeiten

BK: Die BK erstellt gegenwärtig den Bericht in Erfüllung der Postulate 17.3149 Hausammann[21], und 17.4017 Müller Damian[22]. Dieser Bericht wird unter anderem aufzeigen, welche Rolle der Bund bei der Förderung von digitalen Beteiligungsinstrumenten spielen kann und soll. Wir haben bisher kaum Anzeichen dafür gefunden, dass für Plattformen zur Online-Deliberation eine grosse ungedeckte Nachfrage besteht. Der Bericht sollte vom Bundesrat bis Mitte 2019 verabschiedet werden.

EDA: Diese Thematik betrifft auch die Auslandschweizerinnen und Auslandschweizer. Eventuell ergeben sich Synergien mit den Arbeiten an der Massnahme «Weiterentwicklung der Demokratie auf Basis einer digitalen Selbstbestimmung» unter Federführung des EDA im Rahmen der Strategie «Digitale Schweiz».

[21] Postulat 17.3149 Hausammann Markus vom 16.03.2017 Vernehmlassungsverfahren vereinheitlichen und effizienter machen, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173149

[22] Postulat 17.4017 Müller Damian vom 04.12.2017 Die Chancen von Civic Tech nutzen, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017

4 Abkürzungsverzeichnis

Abs.	Absatz
ABU	Allgemein bildender Unterricht
AGB	Allgemeine Geschäftsbedingungen
ASP	Abteilung Sicherheitspolitik (im EDA)
BBl	Bundesblatt
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
Bst.	Buchstabe
BWL	Bundesamt für wirtschaftliche Landesversorgung
CYD	Cyber-Defence, Verteidigung im virtuellen Raum
DV	Direktion für Völkerrecht (im EDA)
EDA	Eidg. Departement für auswärtige Angelegenheiten
EDI	Eidg. Departement des Innern
E-DSG	Datenrecht
EFD	Eidg. Finzanzdepartement
E-Gov	Electronic Government, elektronische Behördendienstleistungen
E-ID Gesetz	Elektronische Identifizierung
EJPD	Eidg. Justiz- und Polizeidepartement
EPFL	Ecole polytechnique fédérale de Lausanne
ETHZ	Eidg. Technische Hochschule Zürich
EU	Europäische Union
E-Voting	Electronic Voting, elektronisches Wählen und Abstimmen
Fablab	Fabrication Laboratory, Fabrikationslabor, digitale Werkstatt
FF	Federführung
FUB	Führungsunterstützungsbasis der Armee

Gov Lab	Governance Laboratory, Innovationslabor für den öffentlichen Sektor
GPK-S	Geschäftsprüfungskommission-Ständerat
HR	Human Resources
IGE	Institut für Geistiges Eigentum
IKT	Informations- und Kommunikationstechnik
KGSi	Kerngruppe Sicherheit
KI	Kritische Infrastruktur
MELANI	Melde- und Analysestelle Informationssicherung
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NDA	Non-disclosure Agreement, Geheimhaltungsvereinbarung
NFP	Nationales Forschungsprogramm
ODR	Online Dispute Resolution, Online-Beschwerde und Streitschlichtungsmechanismen
Pa. Iv.	Parlamentarische Intervention
PBV	Preisbekanntgabeverordnung
Q	Quartal
RK-S	Kommission für Rechtsfragen - Ständerat
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SCION	Scalability, Control and Isolation on Next Generation Networks
SECO	Staatssekretariat für Wirtschaft
SEV 218	Übereinkommen des Europarats über einen integrierten Schutz, Sicherheit und Service-Ansatz bei Fußballspielen und anderen Sportveranstaltungen
SiA	Sicherheitsausschuss des Bundesrates
SIPOL	Sicherheitspolitik der Schweiz
SNF	Schweizerischer Nationalfonds
SR	Ständerat
StGB	Strafgesetzbuch

TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights, Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums
UID	Unternehmens-Identifikationsnummer
UVEK	Eid. Departement für Umwelt, Verkehr, Energie- und Kommunikation
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport
WBF	Eidg. Departement für Wirtschaft, Bildung und Forschung