www.jusletter-it.eu

Sandra Husi-Stämpfli / Peter Andres

# Die Wolke lockt: Digitale staatliche Souveränität in Bedrängnis

## Der Gang in die Cloud fordert das Konzept der digitalen staatlichen Souveränität heraus

Die Diskussion um den Einsatz von Cloud-Dienstleistungen in der öffentlichen Verwaltung entwickelt sich je länger je mehr zu einer Gretchenfrage: «Sag, wie hast du's mit der Cloud?» Oder genauer: «Wie hast du's mit den Herausforderungen, die mit einer Cloud-Lösung einhergehen?» Da sind auf der einen Seite die unbestreitbaren Vorteile, die Cloud-Services für (kantonale oder Bundes-)Organe mit sich bringen: Hohe und insbesondere stabile Rechenleistung kann vergleichsweise günstig und je nach Bedarf eingekauft werden. Ein fast unschlagbares Argument, wären da nicht die auch bei Cloud-Services unvermeidbaren Sicherheitsrisiken aufgrund von Cyberattacken, die rechtlichen Herausforderungen von Auftragsdatenbearbeitungen und Datenbearbeitungen im Ausland und schliesslich eben die staats- und gesellschaftspolitischen Fragen zur digitalen staatlichen Souveränität. Gerade im Hinblick auf die staatliche digitale Souveränität zeigt sich aber, dass die Auseinandersetzung mit der Thematik noch in den Kinderschuhen steckt: Es scheint fast, als würde die Relevanz von Daten für das Funktionieren des Staates und die innere Sicherheit unterschätzt, weil Daten eben «nicht greifbar» sind – ganz im Gegensatz beispielsweise zu den staatlichen Goldreserven, deren Schutzbedarf und deren inländische Lagerung niemand bestreitet. Sandra Husi und Peter Andres greifen diese Themen in ihrem Beitrag auf und ordnen die Risiken der Cloud-Nutzung im staatlichen Kontext sowohl in staatspolitischer, rechtlicher wie auch in technischer Hinsicht ein: Eine einfache «schwarz/weiss Lösung» kann es auch im Cloud-Kontext nicht geben, weshalb die Autorin und der Autor Denk- bzw. Lösungsansätze aufzeigen, wie Entscheidungsträger ihrer Verantwortung im Cloud-Umfeld gerecht werden können.

Beitragsart: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Sandra Husi-Stämpfli / Peter Andres, Die Wolke lockt: Digitale staatliche Souveränität in Bedrängnis, in: Jusletter IT 26. April 2022

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

## Inhaltsübersicht



## I. Einleitung[1]

[1] Am 7. März 2021 hat das Schweizer Stimmvolk das Bundesgesetz über elektronische Identifizierungsdienste deutlich mit 64.4 % der Stimmenden abgelehnt, kein einziger Kanton hat der Vorlage zugestimmt. Die Gründe dafür sind mannigfaltig, jedoch wurde ein zentraler Punkt von den Gegnern des Gesetzes immer wieder betont: «*Die Herausgabe von Identitätsausweisen muss in staatlicher Verantwortung bleiben und gehört unter demokratische Kontrolle*». Den Gegnern war wichtig, dass

- die Datenhoheit und somit die Daten selbst vollumfänglich in staatlicher Verantwortung bleiben müssen, denn eine E-ID sei nur dann vertrauenswürdig, wenn sie staatlich ist;
- dass der Datenschutz ein elementarer Aspekt der Lösung und sehr hoch sein soll, und dass
- die (informationelle) Selbstbestimmung zentral ist.[2]

[2] Unter keinen Umständen sollten die Daten von einem Privaten «verwaltet» werden. Diese Forderungen wurden nach der Abstimmung von sämtlichen Fraktionen in gleichlautenden Motionen erneut bekräftigt.[3]

[3] Aber nicht nur die *individuelle* digitale Souveränität hat ihren Eingang in den gesellschaftlichen Diskurs gefunden, auch die Themen der Cybersecurity und der staatlichen Aufgaben in der digitalisierten Gesellschaft drängen ins Bewusstsein der Bevölkerung: Eine im Januar 2022 veröffentlichte Studie der SWICO[4] hat ergeben, dass die Bevölkerung eine Intensivierung der staatlichen Bemühungen erwartet, um die Grundbedürfnisse nach digitaler Bildung, sowie insbesondere zum Schutz vor digitaler Gewalt, und der Gewährleistung der Cybersicherheit professionell und mit hoher Kompetenz anzugehen. Der digitale Wandel hat dazu geführt, dass die

1 Die Autorin und der Autor geben in diesem Beitrag ihre persönliche Meinung wieder.

2 Das Referendumskomittee hat seine Gegenargumente unter https://www.e-id-referendum.ch/argumente zusammengefasst.

Diese und die nachfolgenden Internet-Quellen wurden das letzte Mal am 24.03.2022 kontrolliert.

3 Motionen 21.3124, 21.3125, 21.3126, 21.3127, 21.3128, 21.3129 «Vertrauenswürdige staatliche E-ID», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213124.

4 Studie «Digitaler Staat in der Schweiz, Einschätzungen und Bedürfnisse der Bevölkerung, Januar 2022», durchgeführt von SOTOMO im Auftrag der SWICO, abrufbar unter: https://www.swico.ch/media/filer_public/99/19/9919fe71-b4c7-4024-bc6a-e1aa9743c06f/sotomo_swico_digitaler_staat.pdf?vgo_ee=FQkJhwU4Mu1Ew7yl4DU8sE5I2jKxc%2Bu7z1tNMUbX0LI%3D.

grundlegendste staatliche Funktion überhaupt – Sicherheit für seine Bürgerinnen und Bürger zu schaffen – aus Sicht dieser Bürgerinnen und Bürger auch zu einer Kernaufgabe des digitalen Staats geworden ist. Das Aufkommen dieses Verständnisses bzw. dieser Forderungen in unserer breiten Gesellschaft ist erfreulich, darf aber nicht darüber hinwegtäuschen, dass sich die Wahrung der Sicherheit in der digitalisierten Gesellschaft nicht nur unmittelbar auf die Bedürfnisse der oder des Einzelnen beziehen kann. Vielmehr erstreckt sich die Thematik deutlich weiter, bis hin zur sogenannten digitalen staatlichen Souveränität: Digitale Souveränität beschreibt die Fähigkeit zur Selbstbestimmung in der digitalen Welt. Sie beinhaltet die Wahl- und die Handlungsfähigkeit, die nachhaltige Sicherstellung des freien Marktes, die Datensouveränität und die Cybersicherheit sowie Vermeidung der Abhängigkeit bei digitalen Kerntechnologien von Drittstaaten. Die Pandemie hat einmal mehr gezeigt, dass der Staat seine hoheitlichen Aufgaben auch in Zeiten zunehmender Digitalisierung erfüllen können muss.[5]

[4] Es erstaunt daher auch nicht, dass Parlamentarierinnen und Parlamentarier[6] fordern, dass der Bund eine angemessene digitale Infrastruktur baut, welche die Basis der digitalen Souveränität der Schweiz bilden kann. Dabei geht es darum, digitale Infrastrukturen, unabhängige Cloudplattformen und selbstverwaltete Rechenzentren mit gesicherten Daten in der Schweiz, welche zu einer solchen Souveränität beitragen können, zu schaffen. Der Bundesrat ist sich dieser Problematik bewusst und beantwortet die Motion damit, dass im Rahmen der Umsetzung der bestehenden Strategien ebenfalls geprüft wird, ob und wo zusätzlich technische Lösungen nötig sind, um die Sicherheit im digitalen Zeitalter zu gewährleisten.

[5] Wie passen nun diese Forderungen des Volkes und des Parlamentes bzw. die Aussagen des Bundesrates zu den Bemühungen der Bundesverwaltung, vermehrt auf kommerzielle Cloud-Services zu setzen? Die Public Cloud-WTO-Ausschreibung[7] mit einem Volumen von über CHF 100 Mio. haben Hersteller aus den USA, Europa und China gewonnen, keiner aus der Schweiz[8]. Das heisst, der Schweizer Staat wird künftig zumindest einen Teil seiner Daten auf Infrastrukturen der Unternehmen Alibaba, Amazon, IBM, Microsoft oder Oracle betreiben. Und auch die IKT-Teilstrategie Büroautomation der Bundeskanzlei sieht vor, diese künftig ganz oder teilweise in einer Cloud zu betreiben. Dazu wurde das Projekt Cloud Enabling BüroAutomation (CEBA)[9] gestartet. In letzter Konsequenz heisst das, dass bei einem CEBA-Ansatz die Daten der Büroautomation sowohl in den flüchtigen (dem sog. Memory), als auch in den physikalischen Speichern der Cloudanbieter bearbeitet werden.

[6] Und wie passt der Gang in die Cloud zu den deutlichen Berichten[10] von MELANI[11], wonach die Gefahr durch Hackerangriffe nicht nur real ist, sondern sogar laufend zunimmt, insbesondere auch gegen Regierungen bzw. öffentliche Verwaltungen? Wie ist der Umstand zu beurteilen, dass

5 https://www.stmd.bayern.de/wp-content/uploads/2021/10/Positionspapier-der-L%C3%A4nder-souver%C3%A4ne-deutsche-Verwaltungscloud.pdf.

6 Motion 19.3884 Derder, «Eine Strategie für die digitale Souveränität der Schweiz», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193884.

7 Abrufbar unter https://www.it-beschaffung.ch/it/1202937/20007-608-public-clouds-bund.

8 Siehe dazu die kritische Berichterstattung von Adrienne Fichter in der Republik vom 14.01.2022, «Wie wegen einer Wolke alle in die Luft gehen», wonach der Datenschutzthematik bei der Beschaffung zu wenig Aufmerksamkeit geschenkt wurde, https://www.republik.ch/2022/01/14/rekonstruktion-des-cloud-dramas.

9 https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/bueroautomation.html.

10 https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html.

11 Melde- und Analysestelle Informationssicherung.

die Angriffe dabei vor allem gegen virtualisierte und cloudbasierte Infrastrukturen erfolgen, und zwar sowohl auf der Software- wie auch der Hardware-Ebene?

[7] Der vorliegende Beitrag beleuchtet neben den juristischen Fragestellungen rund um den Einsatz von cloudbasierten Infrastrukturen in der öffentlichen Verwaltung auch die technische Sichtweise: Wie sicher sind diese Cloud-Dienste und Cloudinfrastrukturen – und wie lässt sich der staatliche Gang in die Cloud mit den Forderungen (und dem Bedarf?) nach digitaler staatlicher Souveränität vereinbaren?

## II. Rechtliche Einordnung: Der Staat in der Cloud – nichts anderes als eine Auftragsdatenbearbeitung?

### 1. Die Theorie: Vorgaben nach Datenschutzrecht

[8] Das Bundesgesetz vom 25. September 2020 über den Datenschutz,[12] welches immer dann zur Anwendung gelangt, wenn Bundesorgane[13] (besonders schützenswerte) Personendaten[14] bearbeiten,[15] enthält als technikneutrales Gesetz keine Vorgaben, die die Cloud-Thematik explizit adressieren. Vielmehr muss die Nutzung von Cloud-Infrastrukturen unter das allgemeine Gefüge der Datenschutzvorgaben subsumiert werden. Für die Bundesverwaltung bedeutet dies Folgendes:

#### 1.1. Auftragsdatenbearbeitung inkl. Verantwortung

[9] Sofern Personendaten mittels Cloud-Infrastrukturen bearbeitet werden sollen – «Bearbeiten» im datenschutzrechtlichen Sinne enthält sämtliche Vorgänge, vom Beschaffen über das Verwenden bis hin zum Archivieren und Löschen[16] – muss aus datenschutzrechtlicher Sicht von einer «Datenbearbeitung durch Dritte» bzw. einer Auftragsdatenbearbeitung im Sinne von Art. 9 DSG[17] ausgegangen werden.

[10] Derartige Auftragsdatenbearbeitungen sind zulässig, sofern direkt in einem Gesetz oder, was im Kontext des Cloud-Computings der Normalfall sein dürfte, mittels Vereinbarung sichergestellt wird, dass die beauftragte Person (in casu der Cloud-Service-Anbieter) die Daten nur so bearbeitet, wie dies die Auftraggeberin (die Cloud-Nutzerin, d.h. das fragliche Bundesorgan) dies selbst tun dürfte (Art. 9 Abs. 1 lit. a DSG). Zudem darf weder eine gesetzliche noch vertragliche Geheimhaltungspflicht der Auftragsdatenbearbeitung entgegenstehen (Art. 9 Abs. 1 lit. b DSG).

---

12 DSG, SR 235.1. In diesem Beitrag wird bereits auf das neue Datenschutzgesetz verwiesen. Divergieren die Bestimmungen des «neuen» Datenschutzgesetzes mit jenen des zum Zeitpunkt der Publikation noch geltenden «alten» Datenschutzgesetzes vom 19. Juni 1992, so werden die entsprechenden Nachweise und Unterschiede jeweils in einer Fussnote aufgeführt, wobei das «alte» Datenschutzgesetz mit «DSGalt» abgekürzt wird.

13 Der Begriff des Bundesorgans ist unverändert geblieben: Art. 6 lit. i DSG.

14 Art. 5 lit. a und c DSG – vergleiche zum Begriff der besonders schützenswerten Personendaten das alte DSG: Art. 3 lit. c DSGalt.

15 Der Begriff des Bearbeitens ist unverändert geblieben: Art. 5 lit. d DSG.

16 Siehe Fn. 15.

17 Vormals Art.10a DSGalt. Die Bestimmung wurde inhaltlich unverändert übernommen bzw. lediglich redaktionell angepasst.

[11] Die Verantwortung für die bearbeiteten Personendaten verbleibt auch bei einer Auftragsdatenbearbeitung bei der Auftraggeberin,[18] dem ursprünglich verantwortlichen Bundesorgan. Das A und O der Auftragsdatenbearbeitung – und damit des Cloud-Computings – ist somit das Vertragswesen: Der Cloud-Service-Anbieter muss verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten und dabei insbesondere die Vorgaben zur Datensicherheit (nachfolgend Ziff. 1.3) und zu den Rechten der betroffenen Personen (nachfolgend Ziff. 1.4). Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Anbieter beigezogen werden.

### 1.2. Datenbekanntgabe ins Ausland

[12] Entscheidet sich ein Bundesorgan, mit einem Cloud-Service-Anbieter zusammenzuarbeiten, so muss geprüft werden, ob die Daten im Ausland bearbeitet bzw. gespeichert werden. In diesem Fall müssen zusätzlich zu den Vorgaben zur Auftragsdatenbearbeitung auch die Rahmenbedingungen für die Datenbekanntgabe ins Ausland eingehalten werden (Art. 16 DSG): Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet[19] – liegt kein solcher Angemessenheitsbefund vor, so muss der geeignete Datenschutz auf anderem Wege sichergestellt werden. In der Regel[20] wird dies mittels Datenschutzklauseln in einem Vertrag zwischen den involvierten Parteien, d.h. dem Bundesorgan und der Cloud-Service-Anbieterin erfolgen. Wie bereits unter Ziff. 1.1 festgehalten: Die datenschutzrechtliche Zulässigkeit eines Gangs in die Cloud steht und fällt mit dem zugrundeliegenden Vertragswesen bzw. der Präzision und Verbindlichkeit der zwischen den Parteien ausgehandelten Datenschutzklauseln – gerade aber bei Anbietern, die dem US-Cloud Act[21] unterstehen, haben solche Klauseln nur eine beschränkte (Abwehr-)Wirkung.

### 1.3. Datensicherheit

[13] Besonderes Augenmerk bei der Vertragsausgestaltung muss der Datensicherheit sowie der Gewährleistung der Auskunftsrechte der betroffenen Personen (dazu sogleich Ziff. 1.4) gewidmet werden. Die Cloud-Dienstleister müssen verpflichtet werden, die Vorgaben von Art. 8 DSG sowie die Ausführungsbestimmungen in der VDSG umzusetzen.

[14] Der Vertragspartner des Bundesorgans muss die in der Cloud-Infrastruktur bearbeiteten Daten insbesondere vor unbefugter oder zufälliger Vernichtung, bzw. vor zufälligem Verlust schützen und sicherstellen, dass die Daten nicht unbefugt bearbeitet werden. Mit anderen Worten: Vertraulichkeit, Verfügbarkeit und Integrität der Daten müssen sichergestellt werden. Konkret bedeutet dies, dass die via Cloud-Infrastruktur bearbeiteten Personendaten durch angemessene

---

18 Siehe dazu Art. 9 DSG.

19 Art. 16 Abs. 1 DSG. Aktuell findet sich die Liste derjenigen Staaten, die über ein aus Schweizer Sicht angemessenes Schutzniveau verfügen, auf der Homepage des EDÖB: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/20211115_L%C3%A4nderliste_d.pdf.download.pdf/20211115_L%C3%A4nderliste_d.pdf.

20 Art. 17 DSG zählt verschiedene Ausnahmetatbestände auf, die eine Übermittlung von Daten ins Ausland auch ohne Vorliegen einer gesetzlichen Grundlage oder einer vertraglichen Vereinbarung zulassen. Art. 6 DSGalt führte ähnliche Tatbestände auf.

21 Ausführlich dazu der Bericht des Bundesamtes für Justiz vom 17.09.2021, abrufbar unter https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html.

technische und organisatorische Massnahmen geschützt werden müssen, wobei die zu treffenden Massnahmen entsprechend dem Risiko, welches mit der jeweiligen Datenbearbeitung einhergeht, zu wählen sind.

[15] Die Angemessenheit der Schutzmassnahmen bestimmt sich somit nach den Charakteristika der involvierten Parteien (Welche Behörde möchte die Cloud-Services nutzen? Wie ist das Unternehmen organisiert, wo hat es seinen Sitz, seine Rechenzentren?), nach den bearbeiteten Personendaten[22] (wird bspw. ein Personalstamm in einer Cloud bearbeitet, enthält dieser Personalstamm allenfalls Angaben zu verdeckten Ermittlerinnen und Ermittlern?), der gewählten Cloud-Lösung (IaaS, PaaS oder SaaS) usw.

[16] Die Festlegung dieser Aspekte kann jedoch nur erfolgen, wenn die Anwendungsverantwortlichen über das nötige Wissen verfügen, um die von der oder dem Cloud-Anbieter(in) angebotenen Lösungen in technischer und organisatorischer Hinsicht tatsächlich beurteilen und auch abschätzen zu können, welche konkreten Konsequenzen ein Datenverlust nach sich ziehen könnte. Im Sinne des Risiko-Assessments kann immerhin die nachfolgende Faustregel herangezogen werden: Je sensitiver (weil besonders schützenswert), vertraulicher, geheimer oder wichtiger (weil geschäftskritisch) die Daten sind, umso höher die Sicherheitsanforderungen und je strenger die Kontrollmechanismen, insbesondere beim Gang in eine ausländische Cloud.

### 1.4. Gewährleistung der Auskunftsrechte

[17] Nicht nur die Verantwortung (siehe oben Ziff. 1.1) für die in der Cloud bearbeiteten Personendaten verbleibt beim jeweiligen Bundesorgan. Es muss auch dafür besorgt sein, dass die Rechte der betroffenen Personen, d.h. das Auskunftsrecht nach Art. 25 DSG sowie das Recht auf Löschung und Berichtigung (Art. 41 DSG) gewährleistet werden. Nur weil die Daten nicht mehr «on premise[23]» und damit nicht mehr im unmittelbaren Einflussbereich des Bundesorgans bearbeitet (insbesondere gespeichert!) werden, heisst dies nicht, dass sich die betroffenen Personen an die Anbieterin der Cloud-Infrastruktur wenden müssen – ihre Ansprechpartnerin bleibt das jeweilige Bundesorgan.

[18] Für das Bundesorgan, welches eine Cloud-Infrastruktur nutzen möchte, bedeutet dies, dass die Rechte der betroffenen Personen im Vertragswesen festgehalten werden müssen und dass mittels entsprechenden Kontrollmechanismen sichergestellt werden muss, dass diese Rechte auch tatsächlich wahrgenommen werden können. Die Auskunftsgesuche dürfen also nicht ins Leere laufen und die jeweiligen Personendaten müssten auch korrigiert oder allenfalls gelöscht werden können.

22 Dieselben Überlegungen müssten natürlich auch bei der Auslagerung von sensitiven Informationen (ohne Personenbezug, aber z.B. mit Bezügen zur Staatssicherheit) angestellt werden.

23 Die Bezeichnung on premises (oder on Prem) wird verwendet, um ein Lizenz- und Nutzungsmodell für Software zu beschreiben. Software on premises zu betreiben, heisst, sie auf eigenen Servern zu hosten (on premises bedeutet ins Deutsche übersetzt: «in den eigenen Räumlichkeiten»).

## 2. Die Realität

[19] So klar die rechtlichen Vorgaben für den Gang in die Cloud im Grunde wären, so problematisch zeigt sich die Realität, wobei an dieser Stelle nur die wesentlichsten Diskrepanzen beleuchtet werden sollen:

[20] Das Datenschutzgesetz geht davon aus, dass Auftragsdatenbearbeitungen auf vertraglichen Vereinbarungen zwischen mehr oder weniger gleichberechtigten Parteien basieren. Die Verhandlungsposition der Bundesverwaltung (und erst recht eines einzelnen Bundesorgans) gegenüber den «grossen» Cloud-Anbietern ist aufgrund derer Marktmacht jedoch vergleichsweise schwach. Ein eigentliches «Aushandeln» der Cloud-Verträge wird in der Regel nicht auf Augenhöhe der Vertragspartner erfolgen. Sonderlösungen werden von den Anbietern entsprechend ihrer Marktmacht nur bis zu einem gewissen Grad zugestanden («take it or leave it»), und selbst diese unterstehen den Rahmenbedingungen des Cloud-Betriebs: Die Daten werden nicht an einem Standort gespeichert und Subunternehmer sind üblicherweise in die Vertragserfüllung miteinbezogen, womit nicht nur die Transparenz der Datenbearbeitungsvorgänge leidet: Auch das eigentlich erforderliche angemessene Schutzniveau dürfte aufgrund dieser Rahmenbedingungen oftmals unterschritten werden.

[21] Selbst wenn somit ein «Cloud-Vertrag» ausgehandelt wird, so wird die Cloud-Nutzerin, d.h. das Bundesorgan, ihre datenschutzrechtlichen Pflichten hinsichtlich der Gewährleistung der Datensicherheit, der Gewährung des Auskunftsrechts oder der Berichtigung und Löschung der Daten faktisch nicht (mehr) oder nur ungenügend wahrnehmen können. Von den anderen Compliance-Vorgaben ganz zu schweigen: Bundesorgane unterstehen ja nicht nur dem Datenschutzrecht, auch Aufbewahrungs- und Beweisvorschriften sowie zahlreiche gesetzliche Geheimhaltungsvorschriften sind – auch beim Gang in die Cloud – zu wahren.

[22] Und schliesslich wäre da aus rechtlicher Sicht ja auch noch die Frage der fremden Jurisdiktion: Das beste Vertragswerk nützt nichts, wenn die Gesetzgebung desjenigen Staates, in welchem die Daten schlussendlich gelagert werden, einen Zugriff ausländischer (Untersuchungs-)Behörden erlaubt, ohne dass sich die Cloud-Nutzerin gross wehren könnte.[24]

[23] Doch damit nicht genug: Die (rechtlichen) Verantwortlichkeiten der auslagernden Behörde können auch aufgrund von cloud-spezifischen *technischen* Gegebenheiten nicht zufriedenstellend und im Interesse der betroffenen Personen wahrgenommen werden: Da ist einerseits der Umstand, dass Daten, die in eine Cloud ausgelagert werden, oftmals ihre Portabilität bzw. ihre Interoperabilität verlieren, bzw. dass es nur mit sehr grossem Aufwand möglich ist, die Daten auch wieder aus der Cloud «herauszuholen» und in eine andere Infrastruktur zu überführen. Dies hat zur Folge, dass die Personendaten nicht (mehr) oder nur noch mit sehr grossem Aufwand in die eigene IT-Infrastruktur zurückgeführt oder zu einem anderen Cloud-Anbieter migriert werden können. Und andererseits hat die – dem Cloud-Computing oftmals inhärente – fehlende oder mangelnde Abgrenzung der verschiedenen Datenverarbeitungen (sog. Multi-Tenant-Architektur) zur Folge, dass durch Angriffe auf einen Cloud-User auch alle anderen Vertragspartnerinnen und -partner des Cloud-Dienstleisters in Mitleidenschaft gezogen werden können.

[24] Angesichts dieser Gegebenheiten stellt sich tatsächlich die Frage, ob die datenschutzrechtliche Verantwortung, die ein Bundesorgan gegenüber denjenigen Bürgerinnen und Bürgern trägt,

24 Siehe vorne Fn. 21.

deren Daten es bearbeitet, mit dem Gang in die Cloud faktisch überhaupt (noch) wahrgenommen werden kann, und ob sich «der Staat» mit der Auslagerung «seiner» Daten nicht in ein Abhängigkeitsverhältnis begibt, das aus staatsrechtlicher bzw. -politischer Perspektive nicht verantwortet werden kann.

[25] Allerdings darf bei allen rechtlichen Vorbehalten nicht ausser Acht gelassen werden, dass die finanziellen und technischen Vorteile der Cloud im Alltag nicht zu verachten sind: Cloud-Angebote erlauben es, vergleichsweise günstig viel «Rechenpower on demand» zu erhalten, die zudem in hoher Qualität zur Verfügung gestellt werden kann. Gerade für sog. Public Data wie bspw. Geo-Services oder weitere Services *ohne* Personenbezug und *ohne* Konsequenz für die staatliche Souveränität stellen solche Ansätze eine ideale Lösung dar.

[26] Wie sind nun aber diese Vorteile aus *technischer* Risikoperspektive zu beurteilen?

## III. Technische Risikobeurteilung: Was der Gang in die Cloud für den Staat bedeutet

[27] Dass Cyber-Attacken auf staatliche Einrichtungen zunehmen, ist mittlerweile ein bekanntes Phänomen. Die Gründe sind vielfältig:

- Durch die zunehmende Digitalisierung bei staatlichen Stellen wächst zugleich die Anfälligkeit für Cyber-Attacken.
- Bei einem erfolgreichen Angriff besteht ein umfassender und schneller Zugriff auf grosse und unter Umständen sensible Datenmengen (klassifizierte Daten und/oder Daten der inneren Sicherheit der Schweiz).
- Die Anonymität des Internets erschwert die Identifizierung und Verfolgung der Täter.
- Cyberangriffe sind ein für die Täter kostengünstiges Mittel und lassen sich mit relativ hohen Erfolgsaussichten in Echtzeit von überall auf der Welt durchführen.[25]

[28] Studien wie z.B. der 2020 Global DNS[26] Threat Report[27] zeigen, dass heute Cyber-Attacken gegen Behörden längst keinen Einzelfall mehr darstellen, sondern zum Alltag der Behörden gehören. So gaben 78 % der befragten staatlichen Einrichtungen an, bereits Opfer von DNS-Angriffen geworden zu sein, und jede fünfte der befragten Regierungsstellen war mit mehr als zehn Cyber-Angriffen pro Jahr konfrontiert. Die Folgen solcher Cyber-Angriffe sind vielfältig und fatal, sie starten bei klassischen DDos[28] Angriffen, um Daten nicht mehr verfügbar zu machen, reichen über finanzielle Einbussen bis hin zur Gefahr, dass sensitive staatliche Daten Dritten zugänglich gemacht werden und somit Menschen an Leib und Leben gefährdet werden können. Nicht ausser

25 Bundesministerium des Innern und für Heimat, Mehr Angriffe auf Politik, Behörden & Wirtschaft durch Cyber-Spionage, abrufbar unter https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html.

26 Domain Name System.

27 Siehe dazu https://go.crowdstrike.com/global-threat-report-2022.html?utm_campaign=globalthreatreport&utm_content=gtr22&utm_medium=sem&utm_source=goog&utm_term=threat%20report&gclid=CjwKCAiAsYy-RBhACEiwAkJFKop5G7dDfQdtlPNqbufyGTawnKZ1qmPXqd4zbtgCRf-MVgzCOXKSTRBoCyeEQAvD_BwE.

28 Siehe https://www.bsi.bund.de/.

Acht gelassen werden darf in diesem Zusammenhang auch der drohende Verlust des Vertrauens der Bevölkerung in staatliche Institutionen bzw. in deren Umgang mit Daten.

[29] Ein Blick in die MELANI-Halbjahresberichte[29] verdeutlicht, dass auch die Schweiz und deren staatliche Stellen keineswegs von Cyber-Angriffen verschont bleiben. Die Bedrohung aller Bereiche des öffentlichen Lebens und damit unserer staatlichen Souveränität ist durchaus real und erscheint nicht nur in Studien oder Berichten: Im Jahr 2021 wurden mit den Gemeinden Montreux[30], Mellingen[31], Dietikon[32] und Rolle[33] gleich mehrere Schweizer Verwaltungen Opfer von Cyberattacken in diversen Formen. Auffällig war die hohe Zahl an gemeldeten Vorfällen mit Verschlüsselungstrojanern, sogenannter Ransomware, im ersten Halbjahr 2021 (siehe auch MELANI[34]). Schon seit einigen Jahren grassieren solche Verschlüsselungstrojaner als erfolgreiches kriminelles Geschäftsmodell, welches mittlerweile «Ransomware as a Service» (RaaS[35]) eingekauft werden kann.

[30] Da der heutige Trend der Bereitstellung von Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung klar in Richtung «Cloud» resp. «Public Cloud» geht, werden vermehrt auch Cloudprovider Opfer von professionellen Cyber Attacken. So wurde zum Beispiel die Swiss Cloud Computing am 27. April 2021 Opfer eines Hackerangriffes.[36] Dabei schleuste eine unbekannte Täterschaft offenbar die bekannte Ransomware «MedusaLocker[37]» in die Systeme des Unternehmens ein, mit dem Ziel, Lösegeld zu erpressen.

[31] Für solche Angriffe werden oft potentielle Vulnerabilitäten der Systeme oder sogenannte «zero day exploit[38]» ausgenutzt. Häufig sind das Schwachstellen oder Sicherheitslücken in Softwaresystemen, aber nicht ausschliesslich. Dies lässt sich anhand verschiedener aktueller Schwachstellen verdeutlichen, welche nicht auf Software- sondern auf Hardwarelücken basieren:

- Bereits im Jahr 2018 wurde die Sicherheitslücke «Meltdown and Spectre»[39] bekannt: Sie betrifft die Hardware und ermöglicht(e) es, nicht-authentisierten Zugriff auf fremde Prozesse und Daten zu erlangen.

29 Siehe dazu https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html.

30 Siehe dazu SRF, Hackerangriff auf die Gemeinde Montreux, Beitrag vom 11.10.2021, abrufbar unter https://www.srf.ch/news/schweiz/cyberkriminalitaet-hackerangriff-auf-die-gemeinde-montreux.

31 Siehe dazu Argovia Today vom 16.11.2021, Mellingen – Hacker-Angriff auf die Gemeindeverwaltung, abrufbar unter https://www.argoviatoday.ch/aargau-solothurn/baden-brugg/hacker-angriff-auf-die-gemeindeverwaltung-144377874?utm_medium=push&utm_source=argoviatoday.ch.

32 Dazu Margrit Keller, Cyberangriffe auf Gemeinden – Spear-Phishing unnötig leicht gemacht?, Economiccrime, Beitrag vom 22.11.2021, abrufbar unter https://blog.hslu.ch/economiccrime/2021/11/22/cyberangriffe-auf-gemeinden-spear-phishing-unn%C3%B6tig-leicht-gemacht/.

33 Yannick Chavanne, Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance, ICTjournal, Beitrag vom 30.08.2021 mit div. Updates, abrufbar unter https://www.ictjournal.ch/news/2021-08-30/cyberattaque-contre-rolle-la-commune-appelle-ses-residents-a-la-vigilance-update.

34 Siehe dazu https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html.

35 Siehe dazu https://www.computerweekly.com/de/definition/Ransomware-as-a-Service-RaaS.

36 Siehe auch https://www.inside-it.ch/post/ransomware-legt-swiss-cloud-computing-und-seine-kunden-lahm-20210429.

37 Siehe dazu https://www.zdnet.de/88371813/medusalocker-neue-ransomware-variante-verbreitet-sich-seit-ende-september/.

38 https://www.kaspersky.de/resource-center/definitions/zero-day-exploit.

39 Siehe dazu https://meltdownattack.com/.

- Im Jahr 2020 wurde die mit einem sog. Base-Score von 9/10 als «critical»[40] eingestufte «RowHammer» Schwachstelle entdeckt: Dabei können mit einem ausgeklügelten Verfahren im flüchtigen Speicher (Memory) benachbarte Speicherbereiche manipuliert werden (sogenanntes Bit-Flipping). Diese Bit-Flippings können dann im Prinzip ausgenutzt werden, um Zugriff auf abgeschirmte Bereiche innerhalb des Systems zu erhalten, ohne dafür irgendeine Software-Sicherheitslücke zu benötigen. So könnte man sich vorstellen, dass auf Cloud-Infrastrukturen, welche von extrem vielen unterschiedlichen Benutzern verwendet werden, Daten eines Bundes-Users ausgelesen werden könnten, wie z.B. seine Session oder ein kompletter RSA-Key.[41]
- Im Jahr 2021 wurde bei der Firma VMWare – einem US-amerikanischen Technologie-Unternehmen und Anbieter von Software-Lösungen im Bereich von Cloud Computing und der Virtualisierung von Rechenzentrumsinfrastrukturen – eine Sicherheitslücke festgestellt, welche mit einem Base-Score von 9.8 (!)[42] beurteilt wurde: Diese Schwachstelle ermöglichte es einem Angreifer, mit dem Hochladen einer Datei direkt auf der Software «vCenter Server» schadhaften Code auszuführen und diesen zu übernehmen. Wiederum sind hier insbesondere virtuelle Infrastrukturen betroffen.

[32] Und schliesslich zeigen die besorgniserregenden Ereignisse in der Ukraine eine weitergehende Dimension der Cyberangriffe: Auch im Cyber-Raum wird Krieg geführt.[43] So wurden (und werden) ukrainische Regierungsstellen, Banken und auch kritische Infrastrukturen gezielt und erfolgreich angegriffen. Gemäss einschlägiger Quellen wurde z.B. eine «Data Wiper» Software in ukrainische Systeme eingeschleust. Also eine Malware, die in einen Rechner eindringt und damit beginnt, Daten zu vernichten. Das Ziel solcher Angriffe ist die absolute Stilllegung der attackierten Infrastruktur.

[33] Ist der Gang in die Cloud damit per se schlecht, unsicher und mit hohen Risiken verbunden – ja gar unverantwortlich? Lässt sich die digitale staatliche Souveränität im Rahmen einer cloudbasierten Infrastruktur gar nicht erst schützen?

[34] Fakt ist zwar, dass cloudbasierte Infrastrukturen aufgrund der hohen Verbreitung und des globalen Einsatzes von virtuellen Systemen ein erhöhtes Risiko für Angriffe bieten. Trotzdem wäre es sicher eine falsche Schlussfolgerung, cloudbasierte Lösungen durchwegs als ungeeignet einzustufen, denn die Cloud-Anbieter arbeiten sehr stark an sicheren Infrastrukturen und sicheren Software-Komponenten. In vielen Umfeldern werden Cloud-Infrastrukturen deutlich sicherer betrieben als kleine «on premise» IT-Infrastrukturen, welche von kleinen Teams mit kleinem Budget betrieben werden. Weiter bieten Cloud-Infrastrukturen sehr viel Computing-Power «on demand», höchste Verfügbarkeit, viele IT- und Infrastrukturdienste per Mausklick zu sehr günstigen Preisen.

[35] Diese Vorteile von Cloud-Infrastrukturen (wie z.B. einer Plattform as a Service PaaS) sollte die öffentliche Verwaltung unbedingt nutzen und gezielt einsetzen – allerdings nicht, ohne

40 Siehe dazu https://nvd.nist.gov/vuln/detail/CVE-2020-10255.

41 Siehe https://arstechnica.com/, https://rambleed.com/docs/20190603-rambleed-web.pdf, https://rambleed.com/.

42 Siehe https://nvd.nist.gov/vuln/detail/CVE-2021-21985.

43 Siehe https://www.it-markt.ch/cybersecurity/2022-02-25/die-moeglichen-folgen-des-cyberkriegs-in-der-ukraine-auf-die-schweiz; https://www.swisscybersecurity.net/cybersecurity/2022-02-24/der-cyberkrieg-in-der-ukraine.

eine sorgfältige Risikoabwägung vorgenommen und spezifische Lösungsansätze evaluiert und realisiert zu haben. So kann man durchaus schützenswerte und vertrauliche Daten der inneren Sicherheit auf Cloud-Infrastrukturen betreiben, jedoch nicht, wenn diese durch private (ausländische) Firmen betrieben werden oder diese mit weiteren Nutzern geteilt werden, wie das z.B. bei der Public Cloud von grossen Providern der Fall ist. In dem Fall verliert der Staat die Herrschaft über die Daten und setzt seine Daten erhöhten Risiken aus.

[36] Zur Erhaltung der staatlichen Souveränität sollten also Cloud-Infrastrukturen von Regierungsstellen für die Regierungsstellen in eigenen Datenzentren betrieben werden – dies sind sogenannte Private Cloud-Infrastrukturen, welche «on premise» betrieben werden. Das Projekt Gaia-x[44] ist eine solche Initiative, welche das Ziel hat, eine sichere europäische Cloud für Regierungsstellen zu bauen.

## IV. Fazit: Die staatliche Souveränität in der Gesellschaft 4.0 – neue Möglichkeiten, verstärkte Verantwortung

[37] Die Speicherung von Daten im Kontext der digitalen Souveränität ist zu vergleichen mit der Lagerung der Goldreserven der Schweiz: Niemand würde auf die Idee kommen, die gesamten Goldreserven in irgendeinem Land in einer Lagerhalle lagern zu wollen, um möglichst viel Geld zu sparen.[45] Vielmehr werden die Goldreserven zu grossen Teilen in einem riesigen atombomben- und einbruchsicheren Hochsicherheits-Tresor im Inneren eines Bergs in einer der bestgeschützten Anlagen der Schweiz gelagert; nur ein kleiner Teil der Goldreserven wird in anderen Ländern gelagert, und selbst dieser Umstand wird immer wieder politisch beanstandet.[46]

[38] Gold hat aber gegenüber Daten einen entscheidenden Vorteil: Es kann nicht kopiert werden, erzählt keine vertraulichen Geheimnisse und lässt sich vergleichsweise einfach ersetzen. Das neue Gold, das neue Geld, sind heute die Daten: Die Daten des Staates, welche letztendlich auch die (digitale) Souveränität ausmachen. Daher ist es unabdingbar, dass mit der digitalen Souveränität des Staates und mit staatlichen Daten immer verantwortungsbewusst umgegangen wird.

[39] Vor dem Gang in die Public Cloud sollte sich das jeweilige (kantonale oder Bundes-)Organ vergegenwärtigen, welche Daten über eine cloudbasierte Infrastruktur bearbeitet werden sollen, wer der Betreiber der entsprechenden Cloud Infrastruktur ist und wo die Daten letztendlich bearbeitet und gespeichert werden. Während öffentliche Meteo-Daten oder allenfalls auch Geo-Daten keine Personenbezüge enthalten und auch die digitale Souveränität eines Staates nicht per se tangieren, dürfte die rechtliche und technische Risikobeurteilung für die Auslagerung von Informationen über die innere Sicherheit eines Staates (bspw. ein Vorstrafenregister, eine Fahndungsdatenbank und polizeiliche Ermittlungssysteme) ein anderes Ergebnis hervorbringen.

---

44 Siehe auch https://www.gaia-x.eu/.

45 Was es bedeuten kann, wenn man die Vermögenswerte nicht in eigenen Händen hält, zeigt aktuell das Beispiel der russischen Zentralbank. Diese verfügt nach eigenen Angaben über Reserven im Gesamtwert von umgerechnet gut 600 Milliarden Dollar. Allerdings lagert ein grösserer Teil dieser Reserven bei westlichen Zentralbanken und Geschäftsbanken. Der jüngsten Statistik zufolge hält die Moskauer Zentralbank Wertpapiere im Volumen von gut 300 Milliarden Dollar im Ausland, welches mittlerweile von vielen Staaten eingefroren wurde, siehe dazu die Reportage von Charlotte Raskopf, «Was die Sanktionen gegen die russische Zentralbank bedeuten» in Capital vom 28.02.2022, abrufbar unter https://www.capital.de/wirtschaft-politik/was-die-sanktionen-gegen-die-russische-zentralbank-bedeuten-31664118.html.

46 Siehe bspw. Ip. 11.3769 Quadri «Goldreserven der Schweizerischen Nationalbank in die Schweiz zurückholen», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20113769.

[40] Die gleichen Überlegungen sollte sich eine Verwaltung auch machen, wenn es darum geht, ganze Informationssysteme mit Personenbezug (bspw. ZEMIS[47] oder RIPOL[48]) oder aber sensible IKT-Infrastrukturen – wie beispielsweise eine PKI[49]-Infrastruktur zum Ausstellen des biometrischen Passes – in eine Public Cloud zu verlagern.

[41] Schliesslich können die Risiken auch versteckt sein: Der Betrieb der Büroautomatisation via Cloud mag vordergründig unproblematisch erscheinen, solange die Informationssysteme mit den Personendaten «on premise» (sprich in den eigenen Räumlichkeiten) gehalten werden. Bei genauerer Analyse wird jedoch rasch deutlich: Wer eine Verfügung bspw. zur Ausweisung einer Person aus Gründen der öffentlichen Sicherheit und Ordnung über ein via Cloud betriebenes Textverarbeitungsprogramm verfasst, riskiert, dass diese Daten von Cloud-Providern und potentiellen Angreiffern mitgelesen werden können.

[42] Neben den softwaretechnischen Sicherheitsmassnahmen macht es aus technischer und sicherheitstechnischer Sicht Sinn, Daten mit hohem bzw. sehr hohem Schutzbedarf auf physikalisch getrennten, stark isolierten Infrastrukturen zu betreiben, welche in der Hoheit des Staates sind. Auch das Bundesamt für Sicherheit in der Informationstechnik BSI empfiehlt entsprechend bei sehr hohen Anforderungen an den Schutzbedarf eine durchgehend physische Separierung der Infrastruktur.[50] Dieser Empfehlung folgt auch MELANI (Zitat: «*we strongly recommend applying some physical segregation for highly sensitive data*»). Solche physikalisch getrennte Architekturen mitigieren das Risiko von Angriffen auf virtualisiere, gemeinsam genutzte Infrastrukturen erheblich.

[43] Diese «on premise» Lösung ist zwar teurer und aufwendiger zu betreiben als der Gang in die Public Cloud, aber dafür eine Lösung, die dem hohen und höchsten Schutzbedarf von Daten der inneren Sicherheit bzw. der digitalen Souveränität der Schweiz gerecht wird[51] – eine Investition, die sich zweifelsohne lohnt und signalisiert, dass Entscheidungsträger bereit sind, ihre Verantwortung in unserer digitalisierten Gesellschaft wahrzunehmen.

---

Sandra Husi, Dr. iur., LLM, Executive MPA Unibe, Leiterin des Stabsbereichs Digital Compliance und Governance des Generalsekretariats EJPD, Datenschutzbeauftragte des EJPD, Bern.

Peter Andres, Ingenieur FH in Mikrotechnik / MAS-IT / EMBA in Innovationsmanagement, CTO ISC-EJPD.

47 Siehe auch https://www.sem.admin.ch/sem/de/home/sem/rechtsetzung/archiv/vo_zemis.html.

48 Siehe auch https://www.fedlex.admin.ch/eli/cc/2016/665/de.

49 Public Key Infrastruktur, dazu die Erläuterungen des BSI unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html.

50 Siehe dazu BSI, Empfehlung: IT im Unternehmen, Server-Virtualisierung, BSI-CS 113 | Version 2.0 vom 11.07.2018, abrufbar unter https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_113.pdf?__blob=publicationFile&v=1.

51 Siehe dazu Bundesministerium für Wirtschaft und Energie, Schwerpunktstudie digitale Souveränität, 2021, abrufbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6.