Johan Christian Clausen Dahl: «Wolkenstudie», 1834. Jörg P. Anders/Staatliche Museen zu Berlin, Nationalgalerie

Zunehmend bewölkt

Hat der Bund aus dem Debakel um die Public-Cloud-Vergabe der Bundeskanzlei gelernt? Auch Swissmedic, die Suva und der Kanton Zürich setzen auf US-Cloud-Giganten. Was sie sich damit einbrocken.

Eine Recherche von Adrienne Fichter, 02.09.2022

Schweizer Behördendaten bei Alibaba, Amazon und Co.? Der Entscheid der Bundesverwaltung im Sommer 2021, bei der Beschaffung einer digitalen Cloud auf chinesische und amerikanische Konzerne zu setzen, sorgte für eine Welle der Empörung.

Verärgerte Parlamentarierinnen, Konkurrenten, eine breite Öffentlichkeit – die Bundeskanzlei und andere beteiligte Bundesämter mussten sich vorwerfen lassen, bei der Cloud-Vergabe Warnungen ignoriert und sogar Rechtswidrigkeiten begangen zu haben.

Die Folgen: eine Untersuchung des Vergabeprozesses durch die Geschäftsprüfungskommission. Eine Beschwerde vor dem Bundesverwaltungsgericht.

Und ein Bürger, der gegen die Public-Cloud-Beschaffung klagt, weil er keine gesetzliche Grundlage dafür sieht. Nach einem Entscheid des Bundesgerichts muss das Bundesverwaltungsgericht nun klären, ob seine Daten vorsorglich geschützt werden müssen, damit sie nicht in der Cloud bearbeitet werden.

Die Bundeskanzlei bemüht sich derweil um Schadensbegrenzung. Und bekannte sich dazu, keine sensitiven Daten wie zum Beispiel Gesundheitsdaten bei Alibaba oder Amazon zu speichern. Ausserdem kommunizierte sie offensiver und forderte in den Verhandlungen für einen Rahmenvertrag von allen fünf berücksichtigten chinesischen und amerikanischen Big-Tech-Konzernen viele Zugeständnisse beim Datenschutz.

Hat der Bund insgesamt also aus diesem Beschaffungsdrama gelernt?

Recherchen der Republik ergeben jetzt:

- Swissmedic, die Zulassungs- und Kontrollbehörde für Arzneimittel, setzt bei ihrer Public-Cloud-Beschaffung ebenfalls auf die US-Anbieter Amazon Web Services (AWS), Oracle und Microsoft. Die Ausschreibungsunterlagen wiesen zum Stand des Datenschutzes in den USA gravierende Mängel auf. Und obwohl es sich um eine wichtige Bundesbeschaffung handelt, ist der eidgenössische Datenschützer nicht in den Prozess involviert worden. Er erfährt durch die Republik-Recherchen vom Zuschlag an die US-Konzerne.
- Trotz derzeit unklarer Rechtslage werden auf kantonaler Ebene Fakten geschaffen. Der Kanton Zürich gab bekannt, seine gesamte Verwaltungsinfrastruktur in die Microsoft-365-Cloud zu verlagern. Der Regierungsrat stützte seine Risikoabwägungen auf eine umstrittene Berechnungsmethode ab. Der Entscheid kommt einem Dammbruch gleich: Mehrere Kantone, etwa Schaffhausen, wollen nachziehen oder prüfen die Option.
- Auch der Unfallversicherer Suva lagert als öffentlich-rechtliche Anstalt gewisse Geschäftsdaten in die Microsoft-365-Cloud aus, wie im Juni durch den eidgenössischen Datenschützer bekannt wurde. Seine Kritik konterte die Suva ihm gegenüber verärgert: Man halte die Methode des obersten Datenschützers zur Einschätzung von Cloud-Risiken «bei allem Respekt für ungeeignet».
- Und auch die Bundeskanzlei steckt weiter in der Zwickmühle: Sie muss die heikle Entscheidung fällen, ob die Microsoft-365-Cloud für die gesamte Bundesverwaltung eingeführt werden soll. Was bisher nicht bekannt war: Beim Bundesparlament ist dies bereits der Fall. Die E-Mails der National- und Ständerätinnen (@parl.ch) befinden sich seit 2021 in Microsoft-Hand.

Swissmedic, der Kanton Zürich, die Suva und auch immer noch die Bundeskanzlei. Bei allen vier Institutionen geht es um dieselben Grundsatzfragen: Lässt das Datenschutzrecht in der Schweiz die Verlagerung von Daten an amerikanische oder andere ausländische Big-Tech-Firmen überhaupt zu? Welche Art von Verschlüsselung ist möglich, um die Daten zu schützen?

Und bei wem liegen dann die Schlüssel?

Weil auch die Europäische Union bis anhin keine verbindlichen Normen verabschiedet hat, die von der Schweiz übernommen werden könnten, treten Schweizer Datenschützerinnen auf die Bremse. Die Ansichten der Datenschutz-Aufsichtsbehörden und der Bundesämter klaffen dabei immer weiter auseinander, der Ton wird zunehmend rauer, die Pattsituation offensichtlicher.

Prescht die Schweiz vor und verlagert sie alle Daten in amerikanische Cloud-Infrastrukturen, könnte dies im Verhältnis zur EU zum dramatischen Nachteil werden: Brüssel könnte den Schweizer Datenschutz als nicht mehr gleichwertig betrachten und die Schweiz wie schon die USA zu einem «unsicheren Drittstaat» herunterstufen. Doch Nichtstun ist für den Bund und die Wirtschaft ebenso wenig eine valable Option. Sie brauchen Rechtssicherheit und solide IT-Infrastrukturen für die Datenverarbeitung.

Ein Dilemma, das jede Institution irgendwie anders löst. Das Resultat: Chaos.

Der Fall Swissmedic. Oder: Wenn schöne Powerpoint-Folien 50-mal wichtiger sind als der Datenschutz

Eigentlich war das Thema am Nachtessen der Parlamentarischen Gruppe Digitale Nachhaltigkeit am Abend des 15. Juni 2022 die bundeseigene Cloud Atlantica. Darüber referierte Dirk Lindemann, der Direktor des Bundesamts für Informatik. Unter den Zuhörern unter anderem die Nationalräte Gerhard Andrey (Grüne), Judith Bellaiche (Grünliberale) und Franz Grüter (SVP).

Doch in der Fragerunde brachte ein Manager des Schweizer Cloud-Anbieters Exoscale ein Beschaffungsgeschäft aufs Tapet, das niemand auf dem Radar hatte: die Public-Cloud-Ausschreibung der Swissmedic vom 4. April 2022.

«Wieder einmal wurden Schweizer Anbieter übergangen, wieder einmal wurden nur amerikanische Hyperscaler berücksichtigt», sagte der Firmenvertreter frustriert. Schweizer Firmen hätten angesichts der kurzen Frist – Abgabetermin war der 16. Mai – keine Chancen gehabt, ein Angebot einzureichen. Zumal der Anforderungskatalog völlig überrissen gewesen sei.

Wer sich die öffentlich verfügbaren Daten zur Public-Cloud-Beschaffung der Swissmedic näher anschaut, stellt tatsächlich fest: Es offerierten lediglich die drei üblichen Verdächtigen. Amazon, Microsoft und Oracle, die Platzhirsche im Cloud-Geschäft, erhielten denn auch den 25-Millionen-Franken-Auftrag (auffindbar unter simap.ch, Projekt-ID : 235296).

Die sogenannten Hyperscaler haben deutliche Vorteile: Sie liefern ihre Leistungen ab Stange und nach Bedarf, sie sind kostengünstig, unschlagbar in Sachen IT-Sicherheit und bieten Technologien an, von denen Schweizer Unternehmen noch weit entfernt sind. Auch Swissmedic will «von diesen Innovationen profitieren und die Vorteile von Public Clouds nutzen», wie die Arzneimittelbehörde die Beschaffung gegenüber der Republik begründet.

Swissmedic hat sich damit wie viele öffentliche Institutionen allerdings ein gröberes Problem eingebrockt: den Datenhunger der Behörden in den USA, wo Oracle, Amazon und Microsoft ihren rechtlichen Hauptsitz haben. Die

Vereinigten Staaten sind 2020 von der EU und der Schweiz offiziell von der Liste der Staaten mit angemessenem Datenschutzniveau gestrichen worden, nachdem sie weitgehende Überwachungs- und Strafverfolgungsgesetze erlassen hatten: den Cloud Act, die Executive Order und die FISA Section 702.

Doch diese grundlegend neue Ausgangslage fand erstaunlicherweise keinen Eingang in die Ausschreibungsunterlagen der Swissmedic. Stattdessen war darin eine veraltete Liste zu finden, auf der die USA noch als Staat mit angemessenem Datenschutz galten. Ein handwerklicher Fehler? «Dass die Liste zur Zeit der Ausschreibungspublikation veraltet war, war nicht bekannt», sagt Eliane Schmid von Swissmedic auf Anfrage der Republik.

Ebenso erstaunlich: Das Thema Datenschutz erhielt in der Ausschreibung als Anforderungskriterium gerade mal 0,2 Prozent Relevanz. Damit wird die Gewichtung und Bedeutung eines Kriteriums abgebildet. Zum Vergleich: Die Präsentationsqualität der offerierenden Firmen wurde mit 10 Prozentpunkten gewichtet. Mit anderen Worten: Schöne Powerpoint-Folien waren 50-mal wichtiger als die Absicherungen, dass US-Behörden keine sensitiven Daten aus der Schweiz in die Hände bekommen.

Besonders pikant dabei: Zwar ist Swissmedic in Organisation und Budget eigenständig, doch handelt es sich um eine öffentlich-rechtliche Anstalt des Bundes. Dennoch wurde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Edöb) nicht in den Beschaffungsprozess involviert, wie er auf Anfrage bestätigt. Vom Zuschlag für Amazon und Co. erfuhr Adrian Lobsiger durch die Republik. Er schreibt auch, dass es keine Hinweise auf eine Datenschutz-Folgenabschätzung «und die damit verbundene Evaluation des Risikos ausländischer Behördenzugriffe» gegeben habe.

Dies bestätigt Swissmedic-Sprecher Alex Josty: «Aktuell ist mit unseren Aktivitäten in der Cloud keine Datenschutzfolgen-Evaluation notwendig.»

Der Fall Swissmedic steht exemplarisch für das Cloud-Drama in Bundesbern, das von einer chaotischen Gleichzeitigkeit des Ungleichzeitigen geprägt ist. Während einige Bundesstellen eigenmächtig vorwärtsmachen und Bedenken in den Wind schlagen, treten Aufsichtsbehörden auf die Bremse. Oft weiss die eine Hand nicht, was die andere tut. Und die Bundesverwaltung befindet sich in einem rechtlichen Vakuum, irgendwo zwischen ewigem Testbetrieb und der definitiven Einführung von Microsoft 365, während die Rahmenverträge mit den ausländischen Cloud-Giganten *«on hold»* sind.

Ein zentraler Aspekt in diesem Cloud-Chaos ist die Frage nach dem Risiko, das amerikanische und chinesische Konzerne mit sich bringen. Dabei stehen sich zwei unversöhnliche Lager gegenüber: die Anwaltsszene und die Zunft der Datenschützerinnen. Sie streiten leidenschaftlich über zwei Kernfragen:

1. Lässt sich das Risiko eines unberechtigten Zugriffs (zum Beispiel von US-Behörden) auf Schweizer Daten in Clouds berechnen?

2. Hilft technische Verschlüsselung gegen solche Zugriffe?

Der Fall Kanton Zürich. Oder: Wie gross ist das Risiko, dass Schweizer Behördendaten in falsche Hände geraten?

Es ist die Gretchenfrage, die alle umtreibt: Lässt sich berechnen, wie hoch das Risiko ist, dass morgen der US-Geheimdienst NSA bei Amazon anklopft und Schweizer Behördendaten anfordert?

Ja, sagen die Privatwirtschaft und viele Juristen, so was lasse sich gut prognostizieren. Nein, das ist Schwachsinn, sagen der eidgenössische und auch einige kantonale Datenschützerinnen.

Das neue Schweizer Datenschutzgesetz erlaubt an sich solche Risikoeinschätzungen, wie auch der Bundesrat in seiner Botschaft festhält. Artikel 16 und 17 regeln die Bedingungen bei einer ausländischen Cloud. Auch die Datenschutz-Grundverordnung (DSGVO) der EU gebietet den Risikoansatz, wie das European Data Protection Board in seinen Empfehlungen festhält.

Doch der eidgenössische Datenschützer Adrian Lobsiger interpretiert das neue Schweizer Datenschutzrecht, das im September 2023 in Kraft treten wird, in Bezug auf ausländische Cloud-Konzerne anders. Für ihn ist klar, dass das Parlament als Gesetzgeber «risikobasierte Abwägungen im Zusammenhang mit Datenexporten in Länder ohne angemessenes Schutzniveau» nicht vorgesehen hat, weder im alten noch im neuen Datenschutzrecht. Deshalb rät Lobsiger dazu, immer von Fall zu Fall nach seiner Anleitung – einem Flussdiagramm – zu prüfen, ob Daten in US-Clouds gelagert werden dürfen.

Der eidgenössische Datenschützer ist aus gutem Grund zögerlich. Über allen aktuellen Cloud-Entscheidungen der Schweiz hängt ein Damoklesschwert: die Anerkennung des Datenschutzniveaus der Schweiz durch die EU, die immer noch aussteht, denn dort stellen sich Lobsigers Amtskollegen inzwischen reihenweise gegen den Ansatz – da soll die Schweiz nicht den Eindruck erwecken, auszuscheren. Auch hat die Schweiz – wie die EU – bis dato kein Nachfolgeabkommen zum für ungültig erklärten Privacy Shield in petto. Dabei handelte es sich um ein amerikanisch-europäisches Datentransferabkommen, das amerikanischen Konzernen wie Facebook, Uber oder Microsoft erlaubt, Daten von europäischen Userinnen legal zu verarbeiten. Im Juli 2020 wurde dieses Abkommen mit dem Schrems-II-Urteil des Europäischen Gerichtshofs zu Fall gebracht. Seither existiert ein fast rechtsfreier Zustand. *Cry and pray* lautet die Losung unter Juristinnen, die versuchen, die Situation für europäische Unternehmen mit komplizierten Vertragsklauseln – und eben Risikobeurteilungen – irgendwie zu überbrücken.

Der Regierungsrat des Kantons Zürich liess sich von diesen Fakten nicht abschrecken: Er beschloss am 30. März dieses Jahres, die Microsoft-365-Cloud-Verwaltungsinfrastruktur einzuführen. Nur sogenannte Geschäftsfalldaten wie etwa Steuerinformationen sowie Daten der Strafverfolgungsbehörden sollen dort nicht gelagert werden. Der Kanton Schaffhausen folgte sogleich, weitere Kantone evaluieren derzeit die Option.

Der 12-seitige Regierungsratsbeschluss ist bemerkenswert, denn er liest sich wie eine Hochglanzverkaufsbroschüre des US-Cloud-Konzerns. Darin ist von «geringer Zukunftsfähigkeit» die Rede, sollte nicht eine Microsoft-Cloud eingeführt werden. Ausserdem würde die «Arbeitgeber-

attraktivität leiden», und der Kanton würde sich «technologisch ins Abseits manövrieren». Mit anderen Worten: Microsoft ist für den Zürcher Regierungsrat alternativlos.

Interessant dabei: Dem Beschluss ging die Anwendung der populären Methode des bekannten Zürcher Juristen David Rosenthal voraus. Dabei handelt es sich um ein Excel-Sheet mit allerlei Formeln, mit denen sich die Wahrscheinlichkeit des Datenzugriffs durch die NSA, das Department of Justice und andere US-Behörden auf Kommazahlen genau berechnen lässt. Die Idee: Man dekliniert technische und rechtliche Sachzwänge durch. Wie zum Beispiel die «Wahrscheinlichkeit, dass die Daten Inhalte umfassen, die Gegenstand von nachrichtendienstlichen Suchaufträgen aus dem betreffenden Land sind».

In einem Workshop mit Vertreterinnen des Amts für Informatik, der Staatsanwaltschaft, der Kantonspolizei und der Staatskanzlei kam der Kanton Zürich zum Schluss, dass die Wahrscheinlichkeit einer erfolgreichen «Datenausbeute» der US-Behörden sehr gering sein wird. Im Klartext: Laut den Excel-Berechnungen der Zürcher Vertreter komme es nur alle 1206-Jahre zu einem erfolgreichen *lawful access* durch die US-Behörden.

Das geht aus einer Dokumentation hervor, die der Republik vorliegt.

Ich will es genauer wissen: Die Methode zur Risikoberechnung eines Schweizer Juristen als globale Erfolgsgeschichte

Juristen mögen keine Zahlen, wie ein Berner IT-Anwalt sagt. Und doch sei die Methode des Zürcher Juristen David Rosenthal äusserst populär. Eine Anwältin, die wie viele andere in dieser Recherche nicht genannt werden will, sagt: «Das Tool dient vor allem als Dokumentation, um gegenüber Aufsichtsbehörden etwas vorweisen zu können und Klientinnen etwas anzubieten, mit dem sie arbeiten können.» In der Tat scheint die Methode Rosenthal global Schule zu machen: Sie gilt seit 2020 als Benchmark im Finanzsektor, wurde von der Zürcher Kantonalbank angewandt und auch von der International Association of Privacy Professionals übernommen. Die Videokonferenzsoftware Zoom hat auf der Basis von Rosenthals Methode eigene Berechnungen für den Datenzugriff der Justizbehörden vorgenommen. Und auch die holländische Regierung hat bereits damit gearbeitet, obschon deren Justizbehörde besonders viel Druck auf US-Konzerne ausübt. Und eben auch die Suva, die nicht mit der Anleitung des eidgenössischen Datenschützers (Edöb) arbeitete, sondern mit Rosenthals Excel-Datei. Dabei kam das Resultat heraus, dass es statistisch gesehen nur alle 903 Jahre zu einem erfolgreichen Herausgabebefehl von Daten kommen werde *(«lawful access»).*

Der eidgenössische Datenschützer hält von solchen Wahrscheinlichkeitsrechnungen nicht viel. In der Stellungnahme vom 14. Juni 2022 zur Cloud-Vergabe der Suva an Microsoft hält Adrian Lobsiger fest: «Dieser Anspruch auf Wertgenauigkeit weckt Zweifel.»

Der Urheber der Risiko-Exceltabelle kann wenig mit dieser Kritik anfangen. Prozentangaben seien viel klarer als irgendwelche Wischiwaschi-Formulierungen, sagt David Rosenthal der Republik. «Meine Methode bietet keine Kristallkugel, sondern einen strukturierten und transparenten Risikobeurteilungsprozess (...). Die Zweifler sollten zeigen, wie sie es besser machen würden.»

Die Swissmedic hat zwar nicht mit der Methode Rosenthal gearbeitet. Doch auch die Arzneimittel-Zulassungsbehörde sieht im amerikanischen Cloud Act «das geringste Risiko». Microsoft könne behördliche Herausgabebefehle juristisch anfechten. Schriftliche Zusicherungen, dass dies auch passiere, habe man allerdings noch nicht. «Die Rahmenverträge sind noch nicht detailliert bekannt und werden erst erarbeitet», sagt Sprecher Lukas Jaggi.

Ausserdem ist Swissmedic der Auffassung, dass sie gar keine Daten besitze, die für die USA von Interesse sein könnten. Die Schweizer Zulassungsgesuche etwa seien auch den amerikanischen und europäischen Pendants bekannt, sagt Eliane Schmid von Swissmedic. «Wir gehen daher davon aus, dass Swissmedic unter keinem im Vergleich zu anderen Zulassungsbehörden erhöhten nachrichtendienstlichen Interesse steht.» (Auch die Suva schreibt sinngemäss in ihrer Stellungnahme zur Microsoft-Cloud, dass ihre Inhalte nicht spannend genug für die NSA seien.)

Wird Swissmedic auch gesundheitsbezogene Personendaten in der Amazon-Cloud verarbeiten? «Das wissen wir noch nicht», sagt Lukas Jaggi. «Besonders schützenswerte Daten werden nicht in der Cloud verarbeitet.» Alles werde im Einzelfall anhand sogenannter Schutzbedarfsanalysen geprüft.

Der Fall @parl.ch. Oder: Wie lassen sich Daten in Clouds vor dem Zugriff ausländischer Geheimdienste schützen?

Der zweite grosse Streitpunkt ist die Frage, ob und wie sich die Cloud-Risiken bei US-Konzernen mit technischen Vorkehrungen minimieren lassen. Können Daten so verschlüsselt werden, dass sie ein Konzern wie Amazon nicht mitlesen kann?

Davon ist man bei Swissmedic offenbar überzeugt: «Durch technische Massnahmen lässt sich weitgehend verhindern, dass der Cloud-Anbieter unkontrolliert Zugriff auf die behördlichen (Klar-)Daten erhält.»

Für viele Kritiker klingt das nach einer Quadratur des Kreises.

Den eidgenössischen Datenschützer stimmen solche Versprechungen sehr skeptisch. Zwar gebe es neue Methoden wie die homomorphe Verschlüsselung – «aber die stecken noch in den Kinderschuhen», sagt Lobsiger. Damit könnten vielleicht «einfache Texte» wie Rechnungen in der Cloud verarbeitet und verschlüsselt werden. Aber bei komplexeren Aufgaben funktioniere «Cloud-Computing» nur, wenn die Cloud-Firmen die Hoheit über die Verschlüsselungen besässen. Dies widerspiegelt in der Tat auch den derzeitigen Stand der Forschung. Auch Lobsigers Kontrahent David Rosenthal räumt dies ein: Ein Cloud-Konzern müsse je nach Anwendungsfall im Besitz der Schlüssel sein, damit dessen Services das tun könnten, «was sie tun müssen».

Theoretisch wäre es möglich, die Schlüssel für die Bundesverwaltung zum Beispiel in einer separaten «Customer-Box» aufzubewahren, auf die Microsoft-Mitarbeitende nicht ohne Erlaubnis zugreifen dürfen – so sieht es der Kanton Zürich vor. Dabei handelt es sich jedoch nur um ein Versprechen des US-Konzerns. Technisch gesehen wäre der Zugriff immer noch möglich.

Wird mit separaten Schlüsselboxen gearbeitet, resultieren auch strengere Auflagen für Angestellte. Wie im Fall des Kantons Zürich: Deren Mitar-

beiterinnen dürfen Steuerdaten via Geschäftsmail, die ebenfalls in der Microsoft-Cloud gehostet werden, zwar versenden. Aber jeder Sachbearbeiter, jede wissenschaftliche Mitarbeiterin muss diese E-Mails vor dem Versand nochmals verschlüsseln. Dabei lauert eine nicht zu unterschätzende Schwachstelle: der vergessliche Mensch.

Extra-Vorsicht müssen seit geraumer Zeit auch Schweizer Bundesparlamentarierinnen walten lassen. Republik-Recherchen zeigen: Die E-Mails von National- und Ständerätinnen (@parl.ch) laufen ebenfalls über die Microsoft-365-Cloud. Die Gruppe Parlaments-IT, eine lose Gruppierung von National- und Ständerätinnen, die sich mit Verwaltungsinfrastruktur auseinandersetzt, liess sich von Microsoft zwar zusichern, dass in jedem Fall rechtlich gegen allfällige Begehren von US-Behörden vorgegangen werden würde; dies geht aus einer Präsentation zur Cloud-Security hervor, die der Republik vorliegt. Doch das Zugriffsrisiko bleibt bei Bundespolitikerinnen bestehen, deren digitale Post für Geheimdienste nicht uninteressant ist.

Die Parlamentsdienste lösen dieses Dilemma mehr schlecht als recht: mit einem Verbot. Kommissionsprotokolle dürfen nicht via @parl.ch-E-Mail an Personen ausserhalb der Bundesverwaltung versendet werden.

So oder so: Die Metadaten – also E-Mail-Betreffzeilen sowie die Namen der Empfängerinnen und Absender – bleiben nicht verborgen, die Microsoft-Mitarbeitenden haben theoretisch darauf Zugriff. Damit erhält Microsoft Personennamen und wichtige Stichworte im Klartext, die problemlos an die Strafverfolgung oder an die Geheimdienste ausgehändigt werden können.

Bei der Microsoft-Cloud sind technische Massnahmen also bloss ein Teil der Lösung. Das Problem lässt sich nur durch vertragliche Zusicherungen der Konzerne einhegen. Oder wie es Jurist David Rosenthal formuliert: Man müsse die Frage stellen, «inwiefern das Anvertrauen des Schlüssels an Provider zu einem *Lawful-access*-Risiko führt».

Ein Tanz auf rohen Eiern

Beide Fronten im Schweizer Cloud-Drama verfolgen berechtigte Anliegen.

Fakt ist: Ohne technologische Infrastruktur aus den USA kommt die Schweizer Wirtschaft zum Stillstand. So gibt es ohne Hyperscaler und ohne Datentransfer ins Ausland zum Beispiel keine internationale Krebsforschung, wie der Anwalt David Vasella schreibt, der zu den Anhängern der Methode Rosenthal zählt und regelmässig auf dem Blog «Datenrecht.ch» publiziert. Auch Swissmedic, Suva und Bundesverwaltung möchten von leistungsstarker Infrastruktur profitieren.

Ein Datenzugriff durch NSA und Co. lässt sich nie völlig ausschliessen oder vertraglich wegbedingen. Die Empfehlung der Anwältinnen an ihre Klienten lautet deshalb: Schliesst mit Microsoft und Co. gute Verträge ab, die euch im Fall des Behördenzugriffs Schadenersatz einbringen. Die Antwort darauf von Datenschützerinnen: Schön und gut, aber dadurch wird der Schaden – die Übergabe von Personendaten – nicht verhindert.

Die Rechtslage bleibt diffus, solange keine verbindliche Rechtsprechung vorliegt. Die Lehrmeinungen, inwiefern der US Cloud Act bei europäischen Ablegern von Oracle, Amazon oder IBM greift, gehen weit auseinander. Solange sich die EU nicht bewegt und der Schweiz die Absolution erteilt, kann

der eidgenössische Datenschützer Lobsiger die Übermittlung von sensitiven Personendaten in US-Clouds nicht bedenkenlos gutheissen.

Und die EU lässt sich viel Zeit damit. Sehr viel Zeit.

Ein Entscheid über die Anerkennung des Schweizer Datenschutzniveaus sollte demnächst vorliegen, wie die Republik in Brüssel erfahren hat: «Die Arbeit der Kommission an diesen Bewertungen ist weit fortgeschritten, und sie beabsichtigt, ihren Bericht in den kommenden Monaten zu veröffentlichen», sagt eine Sprecherin der EU-Kommission. Allerdings: Eine ähnliche Antwort hat die EU-Kommission bereits vor einem Jahr geliefert. Der Fahrplan ist also immer noch unklar – ein Entscheid kann morgen, in ein paar Monaten oder erst im nächsten Jahr gefällt werden.

Der Bundeskanzlei, die federführend für die digitale Transformation der gesamten Bundesverwaltung ist, läuft derweil die Zeit davon. Sie muss zusammen mit dem Bundesamt für Informatik die Public-Cloud-Projekte, die immer noch politischem Widerstand ausgesetzt sind, in trockene Tücher bringen. Das Gerichtsverfahren, in dem die Legitimität der Public-Cloud-Beschaffung angezweifelt wird, könnte zum Abbruch des gesamten Projekts führen.

Die bereits fertigen Rahmenverträge mit Alibaba, Amazon und Co.? Sie würden damit wohl nicht unterzeichnet in der Schublade verschwinden.

Und die Bundesverwaltung muss zusätzlich auch einen Entscheid fällen, was die eigene Verwaltungs-IT betrifft. Denn sie arbeitet ebenfalls mit Microsoft 365, aber bisher eben nur «im Testbetrieb». Darin dürfen «keine besonders schützenswerten Personendaten, keine vertraulichen Dokumente und auch keine Daten (...), die dem Amtsgeheimnis unterliegen», gespeichert werden, wie der Informationsbeauftragte Florian Imbach bestätigt. Lange Zeit schien es nach einer definitiven Einführung auszusehen, schliesslich wurde gemäss dem Fachportal «Inside IT» eine Stelle eines «Business Owner» ausgeschrieben, dessen Aufgabe es gewesen wäre, der «gesamten Bundesverwaltung die zukünftige Nutzung der Cloud Services von Microsoft zu ermöglichen». (Die Stellenausschreibung ist nicht mehr aufgeschaltet.)

Die Bundeskanzlei dementiert solche Gerüchte gegenüber der Republik: «Ein Entscheid über die Einführung von Microsoft 365 wurde noch nicht gefällt», sagt Imbach. Microsoft 365 bleibt also nur ein «Pilotprojekt» der Bundesverwaltung, obwohl bereits Personaldaten von Bundesangestellten im Schweizer Microsoft-Azure-Rechenzentrum gelagert sind.

Eine gute Nachricht gibt es dennoch: Als Folge der Republik-Recherche sollen die Koordination und die Kommunikation bei Cloud-Projekten aller Bundeseinheiten verbessert werden. Daniel Markwalder, der Delegierte des Bundesrates für digitale Transformation, ist vom eidgenössischen Datenschützer kontaktiert worden, um in Zukunft sicherzustellen, «wie Beschaffungsprozesse mit dem geltenden Rechtsrahmen (...) betreffend Datenauslagerungen in Public Clouds in Einklang stehen respektive gebracht werden».

Immerhin!

In einer früheren Version haben wir eine Aussage von David Vasella verkürzt wiedergegeben, sie ist jetzt mit «ohne Datentransfer ins Ausland» ergänzt. Wir bedanken uns für den Hinweis im Dialog.

Und wir schrieben in einer früheren Version, dass die Suva alle Geschäftsdaten in die Microsoft-365-Cloud auslagern wird. Diese Behauptung war abgestützt auf die Korrespondenz

zwischen dem Edöb und dem Unfallversicherer, in der von allen Sparten, Fallmanagement-dokumentationen, Projektunterlagen, E-Mails etc. die Rede war. Nach Angaben der Suva wird dies aber nicht der Fall sein.