Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bern, 31.08.2022

Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung

Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates

Änderungsverzeichnis

Version	Datum	Änderung	Name
0.1		Entwurf 1. Arbeitsgruppensitzung[1]	Ronja Lichtsteiner / Stephan Brunner
0.2	21.1.2022	Überarbeitung, Entwurf für 2. Arbeitsgruppensitzung	Ronja Lichtsteiner / Stephan Brunner
0.3		Überarbeitung nach 2. Arbeitsgruppensitzung, Integration Bemerkungen BJ	Ronja Lichtsteiner / Stephan Brunner
0.4	04.03.2022	Überarbeitung, Integration Bemerkungen EDÖB	Ronja Lichtsteiner
0.5	08.03.2022	Überarbeitung, Integration Bemerkungen Laux-Lawyers AG	Ronja Lichtsteiner / Stephan Brunner
0.6	09.03.2022	Überarbeitung, Integration Bemerkungen DTI	Ronja Lichtsteiner / Stephan Brunner
0.7	18.03.2022	Überarbeitung nach GL BK	Ronja Lichtsteiner / Stephan Brunner
0.8	20.06.2022	Überarbeitung nach DRB	Ronja Lichtsteiner / Stephan Brunner
1.0	16.08.2022	Überarbeitung nach ÄK	Ronja Lichtsteiner / Stephan Brunner
1.1	31.08.2022	Redaktionelle Bereinigung nach Kenntnisnahme GSK	Ronja Lichtsteiner / Stephan Brunner

[1] In der Arbeitsgruppe sind folgende Personen vertreten: Stephan Brunner BK (Leitung); Ronja Lichtsteiner BK; Sandra Husi/ Stephanie Schneiter GS-EJPD; Monique Cossali Sauvain BJ; Monica Ratte GS-EFD; Melanie Koller GS-VBS; Vertreter und Vertreterinnen des EDÖB; Angelika Spiess GS-EFD; Christian Bachofen GS-UVEK; Boris Inderbitzin EDA; Thomas Fischer, Amt für Organisation und Informatik Kanton Bern.

Inhaltsverzeichnis

Anhänge:

Zusammenfassung

Zweck des Berichts

Der Bericht soll zum einen für das Cloud-Sourcing grundlegende Rechtsfragen klären und damit ein für die Bundesverwaltung einheitliches Rechtsverständnis schaffen. Zum anderen soll er aufzeigen, welche Mittel zur Verfügung stehen, um die Zulässigkeit von Cloud-Sourcing-Projekten zu beurteilen und ihre «Compliance» zu gewährleisten. Er soll damit unter anderem auch als Basis für die Rechtsgrundlagenanalyse[2] bei Cloud-Sourcing-Projekten dienen können.

Risikoaspekte (vgl. Teil 1 Risikoaspekte**)**

Abgesehen von der Tatsache, dass die zuständige Verwaltungseinheit nicht mehr selbst die physische Kontrolle über die IT-Mittel hat, tragen insbesondere drei Faktoren zur rechtlichen, aber auch zur technischen Komplexität von Cloud-Sourcing-Lösungen bei, was bei der Risikobeurteilung zu berücksichtigen ist (vgl. Anhänge C bis E):

- Auslandbezug: Aus heutiger Sicht werden insbesondere Public-Cloud-Dienstleistungen von grossen Anbietern (sog. «Hyperscalern») potenziell vollumfänglich oder teilweise im Ausland erbracht (Server-Standorte, Supportzugriffe). Damit muss eine tendenziell abnehmende Kontrolle über das rechtliche Umfeld (z.B. Frage der Angemessenheit der Datenschutzgesetzgebung im Zielland, Risiko von Behördenzugriffen) mit vertraglichen, technischen und organisatorischen Massnahmen kompensiert werden.
- Beizug von Unterauftragnehmern: Für die Auftragserfüllung ziehen Cloud-Service-Provider (auch bei Private-Cloud-Lösungen) in der Regel weitere Dritte bei, die gewisse Aufgaben erfüllen. Diese Unterauftragnehmer erfüllen ihre Aufgaben zudem in manchen Fällen von (weiteren) Drittländern aus.
- Abhängigkeiten von Dritten: Cloud-Sourcing-Lösungen können zu erheblichen Abhängigkeiten von einzelnen Dienstleistern führen, insbesondere was die Verfügbarkeit der Leistungen betrifft.

Welche Restrisiken – in den Grenzen des anwendbaren Rechts – akzeptiert werden können, ist ein– zu fällender Führungsentscheid, der von den Projektverantwortlichen einzuholen ist. Dieser ist ausgehend von der Art der auszulagernden Daten[3] gestützt auf eine Analyse des Rechtsrahmens und einer breiten Risikoanalyse zu treffen. Die Risikoanalyse muss die im konkreten Anwendungsfall bestehenden Risikofaktoren und die Massnahmen zu deren Mitigation berücksichtigen.

Wichtigste Ergebnisse der Analyse zu einzelnen Rechtsgebieten

Datenschutz (vgl. Teil 2 Datenschutzgesetzgebung des Bundes*)*

Die Datenschutzgesetzgebung erlaubt die vertraglich vereinbarte Auftragsdatenbearbeitung durch verwaltungsexterne Dritte. Soweit Auftragnehmende weitere Unterauftragnehmer beiziehen, ist durch entsprechende Vertragsgestaltung und allenfalls auch technische Massnahmen durch die Auftraggebenden sicherzustellen, dass diese an die gleichen Regelungen gebunden sind, wie der Cloud-Service-Provider (nachfolgend auch CSP genannt) selbst (vgl. Teil 2 Ziff. 1.5.1).

Für die Bekanntgabe von Personendaten ins Ausland sieht das Datenschutzgesetz ein differenziertes Regime vor. Eher möglich ist sie, wenn im Zielland eine Gesetzgebung besteht, welche einen angemessenen, der Rechtslage in der Schweiz vergleichbaren Datenschutz gewährleistet. Dies ist insbesondere in der EU und im UK der Fall.

Hinsichtlich der Möglichkeit von ausländischen Behörden, auf Daten zuzugreifen, die sich im Ausland oder unter Kontrolle von ausländischen Auftragsnehmenden befinden, ist eine vertiefte Prüfung im jeweiligen Projekt vorzunehmen. Dies etwa, weil Behörden des betreffenden Staates möglicherweise ohne Kenntnis des Cloud-Nutzers Zugang zu Daten verlangen können oder sich – ohne dass der Cloud-Nutzer die Möglichkeit hat, sich mit Rechtsmitteln dagegen zu wehren – Zugang zu den Daten verschaffen können. Insbesondere für Provider, die US-Gesetzen wie dem CLOUD-Act und FISA Section 702 unterstehen, stellt sich vor diesem Hintergrund die Frage, ob die Rechtsordnung im Land der Dienstleistungserbringung generell besondere Risiken beinhaltet. Für US-Recht kann grundsätzlich von Folgendem ausgegangen werden: Daten von Schweizer Behörden geniessen angesichts der im

[2] Eine Vorlage zur Rechtsgrundlagenanalyse findet sich hier: Rechtsgrundlagenanalyse (admin.ch)
[3] Wo keine Differenzierung aufgrund des Gesetzes nötig wird, werden Daten und Informationen als Synonyme verwendet.

US CLOUD Act enthaltenen Verfahrensmechanismen einen gewissen Schutz vor Datenzugriffen durch US-Behörden, insb. gibt es Hinweise darauf, dass Behördendaten einen höheren Schutz geniessen als private Daten (wenn es auch keine Garantie gibt, dass US-Behörden Schweizer Behördendaten in jedem Fall unberührt lassen). Auch das Risiko von – aus Schweizer Sicht nicht rechtskonformen – Zugriffen gestützt auf FISA und E.O. 12.333 kann auf ein aus rechtlicher Sicht akzeptables Niveau reduziert werden, wenn die im US-Recht bereits vorgesehen Mechanismen mit vertraglichen Vereinbarungen (insb. der Verpflichtung, eine Herausgabe anzufechten) und technischen Schutzmassnahmen ergänzt werden.

Eine entsprechende Prüfung ist im Einzelfall jedoch immer vorzunehmen und muss allenfalls auch politische Risiken einschliessen; das gilt gleichermassen auch für Cloud-Lösungen unter Einbezug von EU-Staaten oder anderen Drittstaaten (vgl. Teil 2 Ziff. 1.6 und Anhang C).

Sofern es um die Bearbeitung von Personendaten geht, gilt es besonders zu betonen, dass eine differenzierte Beurteilung eines konkreten Cloud-Sourcing-Projekts nötig ist. Dabei ist zu berücksichtigen, um welche Art von Daten es geht und auf welche Art und Weise sie bearbeitet werden. Abhängig davon kann beurteilt werden, ob ein die Auslagerung der Daten in die Cloud zulässig ist, und es können die Anforderungen an die organisatorischen und technischen Massnahmen des Datenschutzes festgelegt werden.

Amtsgeheimnis (vgl. Teil 2 Amtsgeheimnis*)*

Cloud-Service-Provider werden im neuen Artikel 320 Ziffer 1 StGB[4] als Hilfspersonen in den Kreis der Amtsgeheimnisträger eingeschlossen. Es können technische Massnahmen getroffen (und vertraglich abgesichert) werden, um einen unrechtmässigen Zugriff auch durch den Cloud-Service-Provider weitgehend zu verhindern, namentlich durch Verschlüsselung oder Pseudonymisierung und Tokenisierung von Daten (vgl. Teil 2 Ziff. 0).

Als Geheimnis gilt jede Tatsache, die nicht offenkundig, noch allgemein zugänglich ist (relative Unbekanntheit) und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat («materielles Geheimnis»; z.B. Informationen, die dem Berufsgeheimnis gemäss Art. 321 StGB unterstehen, spezielle Geheimnisbestimmungen wie Steuergeheimnis, Sozialversicherungsgeheimnis oder korrekt klassifizierte Informationen). Verletzt wird das Amtsgeheimnis, wenn solche Informationen, durch den Amtsgeheimnisträger einem Dritten zugänglich gemacht werden, für welchen diese Information nicht bestimmt ist.

Mit der Einführung des Öffentlichkeitsprinzips in der Bundesverwaltung hat sich der Kreis der Informationen, welche dem Amtsgeheimnis unterstehen (können), bereits reduziert. Grundsätzlich fallen alle Informationen, die nach dem Öffentlichkeitsgesetz bereits zugänglich gemacht worden sind oder nach seinen Regeln ohne Weiteres zugänglich gemacht werden könnten, nicht mehr darunter. Für Personendaten gelten die Regeln des Datenschutzgesetzes, das als Spezialregelung Vorrang hat (vgl. Teil 2 Ziff.1).

Eine Verletzung des Amtsgeheimnisses ist somit primär dann möglich, wenn der (dem Amtsgeheimnis vertraglich unterstellte) Cloud-Service-Provider seinerseits Daten, die unter das Amtsgeheimnis fallen, einem nicht berechtigten Dritten zur Verfügung stellt. Dafür müsste der CSP in der Regel technische Massnahmen umgehen und er würde die vereinbarten vertraglichen Verpflichtungen verletzen sowie allenfalls gegen strafrechtliche Bestimmungen verstossen.

Informationsschutz (vgl. Teil 2 Bestimmungen zum Informationsschutz des Bundes*)*

Auch die geltenden und künftigen Regeln des Informationsschutzes stehen einem Cloud-Sourcing nicht grundsätzlich entgegen. Daten bis und mit Klassifizierungsstufe VERTRAULICH können grundsätzlich durch Auftragnehmende bearbeitet werden, wenn angemessene Massnahmen zum Schutz der Informationen getroffen werden. Die Angemessenheit der Massnahmen hängt unter anderem von der Sensitivität und dem Missbrauchsrisiko sowie dem potenziellen Schaden beim Missbrauch der Daten ab.

Eine Übersicht über die mit Blick auf ein Cloud-Outsourcing zu klärenden Fragen bzw. die zentralen vorzunehmenden Risikoabwägungen findet sich in Anhang D (*Checkliste*).

[4] Voraussichtliches Inkrafttreten am 1.1.2023.

Teil 1 – Vorbemerkungen

1 Einleitung

1.1 Gegenstand und Adressatenkreis

Am 11. Dezember 2020 hat der Bundesrat die Cloud-Strategie der Bundesverwaltung verabschiedet[5] (EXEBRC 2020.2726), welche zum Ziel hat, der Bundesverwaltung den Weg in die Cloud zu ebnen.[6] Aus diesem Grund wurden verschiedene Ziele definiert und in Meilensteine aufgeteilt. Der vorliegende Bericht erfüllt einen Teil von Meilenstein 5 der Cloud-Strategie des Bundes, welcher unter anderem folgendes vorsieht[7]:

«Rechtsklarheit (in Form eines Berichtes) schaffen betreffend die Regelungsinhalte relevanter Rechtsnormen sowie verwaltungsinternen Regelungen, bezogen auf die Nutzung von Public-Cloud-Diensten. Darunterfallen u. a. schweizerische Gesetze (z. B. BWIS, BPG, BPDV Verordnung, PSPV Verordnung, RVOG, ISG, DSG, Strafgesetzbuch, BGÖ), Verordnungen (z. B. ISchV) und IKT-Weisungen aber auch ausländische Rechtsnormen (wie z. B. DSGVO, US CLOUD Act oder Foreign Intelligence Surveillance Act (FISA). Dazu gehören auch Geheimnishaltungspflichten (z. B. Amts-, Geschäfts- und Berufsgeheimnis). »

Das Dokument richtet sich an alle Einheiten der Bundesverwaltung und – neben Juristinnen und Juristen, die sich mit Rechtsfragen im Zusammenhang mit Cloud-Nutzung befassen – insbesondere an führungs- und projektverantwortliche Personen[8], die mit Bezug auf Cloud-Projekte auch für die Berücksichtigung der rechtlichen Aspekte zuständig sind.

1.2 Zweck des Berichts

Dieser Bericht zeigt beschreibend die Rechtsgebiete auf, welche für Cloud-Projekte von Bedeutung sein können und behandelt übersichtsweise die wichtigsten Rechtsfragen. Der Fokus liegt dabei auf dem Datenschutz, der Datensicherheit, dem Informationsschutz sowie dem Amtsgeheimnis. Der Bericht soll zum einen grundlegende Rechtsfragen klären und damit ein für die Bundesverwaltung einheitliches Rechtsverständnis schaffen. Zum andern soll er aufzeigen, welche juristischen Mittel zur Verfügung stehen, um die «Compliance» von Cloud-Sourcing-Projekten zu gewährleisten. Der Anhang C dieses Berichts enthält eine Liste mit Risiken, die beim Cloud-Sourcing vorkommen können und die möglichen Massnahmen, um diese Risiken auf ein akzeptables Niveau zu senken. Diese sollen den einzelnen Verwaltungseinheiten strukturiert aufzeigen, was die sie bei Cloud-Projekten aus rechtlicher Sicht zu beachten bzw. vorgängig zu prüfen haben, um rechtskonform zu sein.

Dieser Bericht beschränkt sich auf Rechtsgebiete, welche die ganze Bundesverwaltung betreffen und geht nicht auf Spezialrecht ein, die sich je nach Sachbereich ergeben können. Der Bericht ist als «living document» zu verstehen: Er soll regelmässig nachgeführt und ergänzt werden.

Die Ergebnisse dieses Berichts haben grundsätzlich für die Rechtsgrundlagenanalyse jedes Cloud-Sourcing-Projekts Gültigkeit, unabhängig vom jeweiligen Modell oder Service.

2 Begrifflichkeiten: Cloud-Modelle und -Services

Um diesen Bericht besser verstehen zu können, werden in diesem Kapitel die Modelle und Services der Cloud kurz vorgestellt. Die Cloudstrategie der Bundesverwaltung sieht fünf Sourcing-Optionen für die Bundesverwaltung vor: Die eigenen Rechenzentren des Bundes (RZ-Bund), die Public Cloud, eine Swiss Cloud, die community-Cloud oder herkömmliches Outsourcing[9]. Auch die Rechenzentren Stra-

[5] Der Bundesrat hat damals entschieden, dass die Cloud relevanten Arbeiten im Programm SUPERB grundsätzlich unabhängig vom Terminplan der Strategieumsetzung fortgeführt werden. Sie werden fortlaufend mit dem Programm SUPERB abgeglichen. Allfällige Diskrepanzen zwischen der Strategie und dem Programm SUPERB werden unter den beiden bereinigt.
[6] Cloud-Strategie der Bundesverwaltung (admin.ch)
[7] Weitere Teilaufträge, insbesondere die Ausarbeitung von Hilfsmitteln, werden im Anschluss gestützt auf den vorliegenden Bericht voraussichtlich bis Ende 2022 erledigt.
[8] Insbesondere auch die Informationssicherheitsbeauftragten des Bundes (ISBD und ISBO).
[9] Siehe Cloud-Strategie der Bundesverwaltung (admin.ch)

tegie des Bundes (RZ-Strategie) sieht vor, dass vermehrt Public Clouds als Rechenzentren genutzt werden sollen.[10]

Heute bestehen auf dem Markt vier Haupttypen von Cloud-Deployment-Modellen[11] und drei Arten von Cloud-Service-Modellen[12].

Die Cloud-Deployment-Modelle lassen sich unterscheiden in:
- Public-Clouds,
- Private-Clouds,
- Hybrid-Clouds und
- Community-Clouds

Die drei Cloud-Services werden wie folgt unterschieden:
- Infrastructure-as-a-Service (IaaS),
- Software-as-a-Service (SaaS) und
- Platform-as-a-Service (PaaS).

Bei den Services geht es um Infrastrukturen, Plattformen oder Software, die dem Cloud-Nutzer über das Internet oder auch dedizierte Verbindungen zur Verfügung gestellt werden. Die Art der Bereitstellung ist das, was die einzelnen Services unterscheidet.

2.1 Cloud-Deployment-Modelle[13]

Public-Clouds

Die Cloud-Infrastruktur wird zur offenen Nutzung durch die Allgemeinheit vom CSP bereitgestellt. Sie kann von einem Unternehmen, einer akademischen oder staatlichen Organisation oder einer Kombination aus diesen bestehen. Sie befindet sich in den Räumlichkeiten des Cloud-Anbieters. Die grössten Anbieter von Public-Clouds sind zum heutigen Zeitpunkt Amazon Web Services, Microsoft und Google.[14]

Private-Clouds

Die Cloud-Infrastruktur wird zur ausschließlichen Nutzung durch eine einzelne Organisation (z.B. Bundesverwaltung) mit mehreren Verbrauchern (z. B. verschiedene Ämter) bereitgestellt. Sie kann sich im Besitz der Organisation, eines Dritten (CSP) oder einer Kombination aus beiden befinden und von diesen verwaltet und betrieben werden, und sie kann «on-premise» oder «off-premise» existieren. Die heutige Atlantica-Cloud des Bundes ist eine solche Private-Cloud.

Hybrid-Clouds

Die Cloud-Infrastruktur ist eine Komposition aus zwei oder mehr verschiedenen Cloud-Infrastrukturen (private, community oder public), die eigenständige Einheiten bleiben, aber durch standardisierte oder proprietäre Technologie verbunden sind, die eine Portabilität von Daten und Anwendungen ermöglicht (z. B. Cloud Bursting zum Lastausgleich zwischen den Clouds).

Community-Cloud

Die Cloud-Infrastruktur wird für die exklusive Nutzung durch eine bestimmte Gemeinschaft oder Gruppe von Verbrauchern aus verschiedenen Organisationen bereitgestellt, die gemeinsame Interessen verfolgen (z. B. Sicherheitsanforderungen, Richtlinien und Compliance-Überlegungen). Sie kann im Eigentum von einer oder mehreren Organisationen in der Gemeinschaft sein, einem Dritten oder einer Kombination von beidem verwaltet und betrieben werden und sie kann «on premise» oder nicht existieren.

[10] Rechenzentren-Strategie Bund (in Bearbeitung).

[12] Siehe oben.
[13] Die Definitionen richten sich nach NIST: NIST SP 800-145, The NIST Definition of Cloud Computing.
[14] Magic Quadrant für Cloud-Infrastruktur und Plattform-Services (gartner.com)

2.2 Cloud-Service-Modelle[15]

IaaS (Infrastructure-as-a-Service)

Bei IaaS wird eine Infrastruktur bereitgestellt, die dem Cloud-Nutzer in der Bereitstellung von Verarbeitungs-, Speicher-, Netzwerk- und anderen grundlegenden Rechenressourcen hilft, auf denen der Cloud-Nutzer beliebige Software, einschliesslich Betriebssystemen und Anwendungen, einsetzen und ausführen kann. Der Cloud-Nutzer verwaltet oder kontrolliert nicht die zugrundeliegende Cloud-Infrastruktur, hat aber die Kontrolle über Betriebssysteme, Speicherplatz und installierte Anwendungen sowie möglicherweise eine begrenzte Kontrolle über bestimmte Netzkomponenten (z. B. Host-Firewalls).

PaaS (Platforms-as-a-Service)

Die dem Cloud-Nutzer zur Verfügung gestellte Produkte besteht darin, in der Cloud-Infrastruktur vom Cloud-Nutzer erstellte oder erworbene Anwendungen einzusetzen, die mit den vom Anbieter unterstützten Programmiersprachen, Bibliotheken, Diensten und Tools erstellt wurden. Der Kunde verwaltet oder kontrolliert nicht die zugrundeliegende Cloud-Infrastruktur, einschließlich Netzwerk, Server, Betriebssysteme oder Speicher, sondern hat die Kontrolle über die bereitgestellten Anwendungen und möglicherweise die Konfigurationseinstellungen für die Anwendungshosting-Umgebung.

SaaS (Software-as-a-Service)

Der Cloud-Nutzer hat die Möglichkeit, die Anwendungen des Anbieters zu nutzen, die auf einer Cloud-Infrastruktur laufen. Der Zugriff auf die Anwendungen erfolgt von verschiedenen Client-Geräten entweder über eine Thin-Client-Schnittstelle, wie z. B. einen Webbrowser (z. B., webbasierte E-Mail) oder über eine Programmschnittstelle. Der Verbraucher verwaltet oder kontrolliert nicht die zugrundeliegende Cloud-Infrastruktur einschließlich Netzwerk, Server, Betriebssysteme, Speicher oder sogar einzelne Anwendungsfunktionen, mit der möglichen Ausnahme begrenzter benutzerspezifischer Anwendungskonfigurationseinstellungen.

3 Risikoaspekte

Die Wahl eines Cloud-Modells bzw. eines genutzten Service in der Cloud, setzt allgemein voraus, dass – unabhängig von den jeweils zu treffenden angemessenen vertraglichen, organisatorischen und technischen Massnahmen – ein minimales Grundvertrauen in die Cloud-Technologie, zum betreffenden Rechtssystem und zum Cloud-Service vorhanden ist, dass die Cloud-Service-Provider sich an Verträge halten und dass sie ihre Systeme nicht zum Schaden der Cloud-Nutzern manipulieren[16]. Dennoch ist für ein konkretes Vorhaben jeweils eine vertiefte und kritische Rechts- und Risikobeurteilung nötig, darauf gestützt sind die erforderlichen Mitigierungsmassnahmen festzulegen (vertragliche, technische oder organisatorische, vgl. Anhang C).

Public-Cloud-Modelle gehen immer mit einer Auslagerung von Daten einher. Daten werden (soweit Infrastrukturen des Cloud-Service-Providers benutzt werden) nicht in eigenen Rechenzentren gespeichert und bearbeitet.

Bei Private-Cloud-Modellen ist ein mögliches Szenario, dass Daten in Rechenzentren bearbeitet werden, die durch Cloud-Service-Provider betrieben, aber ausschliesslich von einem bestimmten Cloud-Nutzer genutzt werden. Auch die Rechenzentren des Bundes fallen grundsätzlich in diese Kategorie, soweit das für die Datenbearbeitung verantwortliche Verwaltungseinheit nicht mit dem Betreiber der Rechenzentren identisch ist[17].

Abgesehen von der Tatsache, dass die zuständige Verwaltungseinheit nicht mehr selbst die physische Kontrolle über die IT-Mittel hat, tragen dabei insbesondere zwei Faktoren zur rechtlichen, aber auch technischen Komplexität dieser Lösungen bei, was bei der Risikobeurteilung zu berücksichtigen ist:

- Auslandbezug: Public-Cloud-Dienstleistungen können sowohl im Ausland wie auch im Inland (Schweiz) erbracht werden (Serverstandorte, Supportzugriffe). Diverse Hyperscaler (z.B. AWS

[15] Die Definitionen richten sich nach NIST: NIST SP 800-145, The NIST Definition of Cloud Computing.
[16] Die Cloud-Service Provider tun dies namentlich, indem sie sich mit entsprechenden Zertifizierungen ausweisen. Vgl. David Rosenthal, Schweizer Banken in die Cloud.
[17] Allerdings sind die rechltichen Rahmenbedingungen andere, insbesondere weil innerhalb der Organisation Bundesverwaltung eine Aufsicht besteht, der Bund die physische Kontrolle über die Infrastruktur hat und die Mitarbeitenden strengeren rechtlichen Bestimmungen unterstehen.

und Microsoft) verfügen über Rechenzentren in der Schweiz. Daher ist es möglich, vertraglich und konzeptionell technisch festzulegen, dass die Datenhaltung und –bearbeitung in der Schweiz zu erfolgen hat (vgl. auch Anhang C).[18]

- Beizug von Unterauftragnehmer: Für die Auftragserfüllung ziehen Cloud-Service-Provider (auch bei Private-Cloud-Lösungen) in der Regel weitere Dritte bei, die gewisse Aufgaben erfüllen[19]. Diese Unterauftragnehmer erfüllen ihre Aufgaben zudem in vielen Fällen von (weiteren) Drittländern aus. Dabei muss die Sicherstellung der Compliance über alle Stellen gewährleistet bleiben.

3.1 Risikoevaluation- und Bewertung

Nicht nur die Nutzung von Public Cloud-Services birgt Risiken. Gewisse Risiken bestehen auch beim herkömmlichen "On-Premise" Modell (bei dem der Betrieb in eigenen Räumlichkeiten, auf eigener Hardware und mit eigenem Personal erfolgt), wie z.B. das Risiko eines Cyberangriffs oder des Ausfalls technischer Infrastrukturen (Bspw. werden Netzwerkinfrastrukturen oft ganz oder teilweise durch Dritte betrieben und/oder gewartet) und damit verbundene Reputationsrisiken sowie die Möglichkeit, dass Daten aus den eigenen Räumlichkeiten entfernt werden[20].

Teilweise werden solche Risiken bei Cloud-Lösungen akzentuiert, unter Umständen aber auch gemildert (ev. besserer Schutz gegen Cyberangriffe[21]). Risiken können mit Cloud-Lösungen aber auch in neuer Weise hinzutreten. Jede Lösung (sowohl eine «On-Premise» als auch Cloud) verlangt, dass – innerhalb des rechtlich zulässigen Rahmens ihre inhärenten Risiken durch geeignete Massnahmen in einem – gegenüber den Vorteilen (z.B. grössere Effizienz, bessere Skalierbarkeit) – verhältnismässigen und damit akzeptablen Rahmen gehalten werden. Dies gilt sowohl für «On-Premise» als auch für Public-Cloud-Lösungen.

Folgende Risikogruppen können grob unterschieden werden:

- Compliance-Risiken (rechtliche Risiken im engeren Sinne): Verletzungen der rechtlichen Vorgaben betreffend Datenschutz, Geheimnisschutz, Informationsschutz, Datensicherheit und weiteren Spezialgesetzen.
- Business-Continuity-Risiken und Disaster-Recovery: Verfügbarkeit des Zugriffs auf eigene Daten, Verfügbarkeit der Netzwerke, Integrität der Daten, Portabilität der Daten (Lock-in Effekte[22]), off the Cloud Backup. Zu beachten sind ggf. auch beschaffungsrechtliche Anforderungen, die dazu führen können, dass Cloud Services nach einer gewissen Zeit gemäss dem Bundesgesetz über das öffentliche Beschaffungswesen (BöB, SR 172.056.1) neu ausgeschrieben werden müssen[23].
- Politische Risiken (vgl. dazu insbesondere auch unten, Teil 2 Ziff. 1.7): Rechtliches Umfeld im Ausland, z.B. Einschränkungen des freien Datenverkehrs; Behördenzugriffe nach ausländischem Recht[24]; nachrichtendienstliche Ausspähung (im In- und Ausland); Konflikte im Ausland.
- Reputationsrisiken: Das Vertrauen der Bürgerinnen und Bürger in die Bundesverwaltung kann je nach Wahl des Cloud-Service-Providers, der in die Cloud ausgelagerten Daten oder möglicher Vorfälle beeinträchtigt werden.

Typische Risiken werden im Anhang C detaillierter aufgezeigt und darauf bezogenen Mitigierungsmassnahmen gegenübergestellt. Aber auch diese können die vorhandenen Risiken in der Regel kaum beseitigen, sondern bestenfalls angemessen reduzieren und für die nötige Resilienz für den Eintrittsfall eines Risikos sorgen.

3.2 Risikoakzeptanz

Welche Restrisiken akzeptiert oder übertragen werden können, ist ein Führungsentscheid der Verwaltungseinheit, die die Verantwortlichkeit über die auszulagernden Daten hat. Dieser ist ausgehend von der Art der auszulagernden Daten gestützt auf eine breite Risikoanalyse in den Grenzen des anwend-

[18] Vgl. dazu insbesondere die Ausführungen unter Ziff. 2.6 unten.
[19] Vgl. NCSC, Merkblatt «Public- oder Hybrid-Cloud-Nutzung in der Bundesverwaltung»,03/2021.
[20] https://www.swissinfo.ch/ger/anklage-macht-ausmass-des-diebstahls-beim-nachrichtendienst-bekannt/42586612, vgl. dazu auch FAQ zum Einsatz von Cloud-Technologien (220826_VUD_FAQ zum Einsatz von Cloud.pdf).
[21] Ob das für ein konkretes Vorhaben gilt, ist im konkreten Fall zu prüfen.
[22] Vgl. NCSC, Merkblatt, Ziff. 3; Millard, S. 43 f.
[23] Für Public-Cloudlösungen unter WTO 20007 ist in diesem Zusammenhang insbesondere zu beachten, dass die Rahmenverträge für eine Zeitdauer von 5 Jahren gelten.
[24] Bisweilen wird dabei von «lawful access» gesprochen.

baren Rechts zu treffen. Die Analyse muss die im konkreten Anwendungsfall bestehenden Risikofaktoren und die Massnahmen zu deren Mitigation berücksichtigen.

Je nach Ergebnis der Risikoanalyse für ein konkretes Vorhaben wird zu entscheiden sein, ob die betreffende Datenbearbeitung in einem Rechenzentrum oder einer Cloud des Bundes, einer anderen, durch Cloud-Service-Provider betriebenen Private-Cloud oder in einer Hybrid-oder Public-Cloud erfolgen kann. Die Darstellung in Anhang E konkretisiert in groben Zügen die Zuordnung von beispielhaften Bearbeitungen zu adäquaten Cloud-Deployment-Modellen.

4 Vertragliche Vereinbarungen mit Cloud-Service-Providern

Die verantwortlichen Stellen der Bundesverwaltung müssen die in den Standardverträgen der Cloud-Service-Providern angebotenen Konditionen sorgfältig daraufhin prüfen, ob diese dem erforderlichen Standard für die zu bearbeitenden Daten entsprechen. Grosse Cloud-Service-Provider («Hyperscaler») verfügen oftmals über komplexe Vertragskonstrukte, welche insgesamt geprüft werden müssen. Dies kann unter Umständen zu einem erheblichen Mehraufwand und einer Umverteilung der Ressourcen (skill-shift) für die betroffene Verwaltungseinheit führen. Gegebenenfalls sind Anpassungen durchzusetzen, insbesondere betreffend die folgenden Punkte (vgl. auch die in Anhang C aufgeführten vertraglichen Massnahmen):

- Überbindung des Amtsgeheimnisses (vgl. Teil 2, Ziff. 0),
- Weisungsgemässe Bearbeitung von Daten (vgl. Teil 2, Ziff. 1.3.2),
- Zusätzliche Sicherheitsmassnahmen (vgl. Teil 2, Ziff. 1.2 und 1.3),
- Kontrollbefugnisse, insbesondere betr. Auditergebnisse (vgl. Teil 2, Ziff. 1.3.2 und 1.5.1).

Auch wenn vertragliche Zusicherungen erwirkt werden können, sind immer auch das Risiko von Vertragsverletzungen und allfällige Hindernisse für deren Aufdeckung durch die Bundesverwaltung in die Risikobeurteilung einzubeziehen.

5 Cloud-Lösungen im Rahmen des Gouvernanzmodells WTO-20007

Das BBL und der Bereich DTI der BK schliessen mit den Zuschlagsempfängern (Cloud-Service-Providern), aus der WTO-Ausschreibung "(20007) 608 Public-Clouds Bund"[25], Rahmenverträge ab über ein gesamtes Dienstleistungsvolumen (Kostendach) von 110 Mio. CHF über 5 Jahre. Die Ausschreibung klammert bestehende Verträge mit Cloud-Service-Providern und Leistungen auf Lizenzbasis aus (d.h. die eine Softwarenutzung umfassen, z.B. Microsoft Outlook M365/CEBA oder SAP Cloud-Lösungen).

Will eine Verwaltungseinheit eine Cloudlösung nutzen, so muss sie im Rahmen eines konkreten Projekts entlang eines anbieterneutralen Pflichtenheftes und vorgegebener Prüfkriterien (z. B.: Erfüllungsgrad der technischen Anforderungen, Konformität zur Cloud-Strategie, Risikobeurteilung [Datenschutz, Informationssicherheit, zugehörige organisatorische- und technische Massnahmen], und einer durchgeführten Evaluation der am besten geeignete Cloud-Anbieter auswählen (die Prüfkriterien müssen sich grundsätzlich nach den Vorgaben im Pflichtenheft der WTO-Ausschreibung richten). Die Verwaltungseinheiten werden entweder selber oder über einen Cloud-Service-Broker (voraussichtlich wird hauptsächlich das BIT diese Funktion wahrnehmen) mit dem betreffenden Cloud-Service-Provider die für das Vorhaben am besten geeignete Lösung auswählen. Grundsätzlich bewegt sich die Auswahl innerhalb der Vorgaben mit dem jeweiligen Anbieter abgeschlossenen Rahmenvertrag. Das abgerufene Volumen wird dem gesamten Dienstleistungsvolumen angerechnet.

[25] Ausschreibungsunterlagen verfügbar unter [werden später publiziert; vgl. auch www.simap.ch; Meldungsnummer 1202937].

Teil 2 – Rechtliche Rahmenbedingungen

Die Nutzung von Cloud-Diensten ist im Grundsatz als administrative Hilfstätigkeit (Bedarfsverwaltung) einzustufen. Als administrative Hilfstätigkeit ist die Beschaffung jener notwendigen Sachgüter oder Leistungen gemeint, die die Verwaltung zur Erfüllung ihrer öffentlichen Aufgabe benötigt.[26] Beispiele dafür sind die Beschaffung von Büromaterial, der Abschluss von Werkverträgen für die Errichtung einer öffentlichen Baute oder eben das Beiziehen eines IKT-Leistungserbringers. Die Verwaltungseinheit schliesst dabei grundsätzlich privatrechtliche Verträge ab. Die gesetzliche Grundlage leitet sich unmittelbar aus der Rechtsgrundlage der jeweiligen öffentlichen Aufgabe ab.[27] Je nach Sachbereich oder Natur der bearbeiteten Daten gelten jedoch spezifischere Anforderungen an die Rechtsgrundlage. Das gilt allgemein namentlich dann, wenn Personendaten Gegenstand eines Cloud-Sourcing sind.

1 Datenschutzgesetzgebung des Bundes

Bei der Bearbeitung von personenbezogenen Daten mit Cloud-Lösungen ist bei vielen Konstellationen davon auszugehen, dass es sich um eine Auftragsdatenbearbeitung im Sinne der Datenschutzgesetzgebung handelt. Soweit also Personendaten in die Cloud ausgelagert bzw. im Rahmen von Cloud basierten Services (insbesondere SaaS-Modell, vgl. Teil 1 Ziff. 2.1) bearbeitet werden sollen, sind die Vorgaben der Datenschutzgesetzgebung einzuhalten.

Das Datenschutzgesetz wurde 2020 totalrevidiert. Das neue Datenschutzgesetz (nDSG) und die dazu gehörenden Verordnungen werden voraussichtlich am 1. September 2023 in Kraft treten.[28] Im vorliegenden Bericht wird weitgehend auf das kommende Recht abgestellt, dessen Anforderungen über das geltende hinausgehen.

Das DSG legt die datenschutzrechtlichen Grundsätze allgemein und technologieneutral fest. Die konkrete Bearbeitung und ihre Rahmenbedingungen werden jeweils im Spezialrecht näher geregelt. Neben dem DSG und dem dazu gehörigen Verordnungsrecht sind daher immer auch datenschutzrechtliche Bestimmungen im Spezialrecht zu berücksichtigen.

Beispiele dafür sind etwa Artikel 58 ff. des Epidemiengesetzes (SR 818.101), Artikel 13 des Bundesgesetzes über kriminalpolizeiliche Zentralstellen, Artikel 60c des Finanzhaushaltsgesetzes (SR 611.0) oder Artikel 55 ff. Energiegesetz (SR 730.0).

Die allgemeinen Grundsätze für die Bearbeitung von Personendaten legt das nDSG in Artikel 6 ff. fest:

- Personendaten müssen rechtmässig bearbeitet werden (die Bearbeitung muss sich insbesondere auf Rechtsgrundlagen mit genügender Normstufe und Normdichte stützen);
- die Bearbeitung muss nach Treu und Glauben erfolgen;
- die Datenbearbeitung muss verhältnismässig sein;
- Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden;
- sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist (Zweckbindungsgebot);
- die Datenbearbeitung ist technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften, insbesondere die Grundsätze nach Artikel 6, eingehalten werden (Art. 9 nDSG).

[26] HÄFELIN/MÜLLER/UHLMANN, Allgemeines Verwaltungsrecht, 8. A., Rz 1384; TSCHAN-NEN/ZIMMERLI/MÜLLER, Allgemeines Verwaltungsrecht, 4. A., Para. 4 N 8 ff.
[27] JAAG führt dazu, unter Hinweis auf die soeben angeführten Autoren, Folgendes aus: «Lehre und Praxis sind sich weitgehend einig, dass für Tätigkeiten im Rahmen der Bedarfsverwaltung eine besondere gesetzliche Grundlage nicht erforderlich ist. Es genügt, dass für die Aufgabe, welcher die Hilfstätigkeiten dienen, eine genügende Rechtsgrundlage vorhanden ist. Mit der Begründung einer Aufgabe wird auch die Kompetenz verliehen, die dafür erforderlichen Mittel zu beschaffen. Das gilt auch für die Kompetenz, die Bereitstellung der erforderlichen Mittel Dritten zu übertragen (Outsourcing).» (ders., Bedarfsverwaltung, in: Sethe et al., Kommunikation. Festschrift für Rolf Weber zum 60. Geburtstag, 543-557, 554).
[28] Referendumsvorlage: BBl 2020 7639; weitere Unterlagen (insb. Vernehmlassungsentwurf zur Verordnung): https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

1.1 Personendaten und Datenbearbeitung

1.1.1 Begriff der Personendaten

Als Personendaten im Sinne des DSG gelten alle Angaben, die sich auf eine bestimmte oder (mit vernünftigem Aufwand) bestimmbare natürliche Person beziehen (Art. 5 Bst. a nDSG). Daten, welche diese Definition erfüllen, dürfen nur unter Einhaltung der datenschutzrechtlichen Vorgaben bearbeitet werden. Insbesondere ist für Bundesorgane eine entsprechende Rechtsgrundlage erforderlich.

Das DSG definiert sodann Kategorien von Daten, bei deren Bearbeitung zusätzlich strengere Anforderungen an die gesetzliche Grundlage gelten, die besonders schützenswerten Personendaten (Art. 5 Bst. c nDSG). In der Regel ist für diese eine Grundlage in einem Bundesgesetz erforderlich. Darunter fallen:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- Daten über die Gesundheit, die Intimsphäre oder
- die Zugehörigkeit zu einer Rasse oder Ethnie,
- genetische Daten,
- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Daten über Massnahmen der sozialen Hilfe.

Etwas strengere Anforderungen sieht das Gesetz für das *Profiling* (vgl. Art. 34 nDSG) vor. Darunter fällt «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen» (Art. 5 Bst. f nDSG).

Profiling mit hohem Risiko ist ein Profiling, das ein hohes Risiko für die Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. (Art. 5 Bst. g nDSG).

1.1.2 «Bearbeiten von Personendaten»

1.1.2.1 Definition «Bearbeiten»

Bearbeiten ist «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, *insbesondere* das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten» (Art. 5 Bst. d nDSG)[29].

1.1.2.2 Voraussetzungen für das Bearbeiten von Personendaten

Für das Bearbeiten von Personendaten genügt in der Regel eine Verordnung als Rechtsgrundlage, es sei denn, es handelt sich um besonders schützenswerte Personendaten. Für deren Bearbeitung ist in der Regel eine Rechtsgrundlage in einem Bundesgesetz nötig (vgl. Teil 1, Ziff. 1.1.1).

Ein *Profiling* ist für Verwaltungseinheiten grundsätzlich nur gestützt auf eine formell gesetzliche Grundlage (Art. 34 Abs. 2 Bst. b nDSG) erlaubt (vgl. auch oben Ziff. 1.1.1). Gesetz im formellen Sinne heisst, dass im Bundesrecht die Stufe des Bundesgesetzes (eine Verordnung reicht nicht aus) erreicht werden muss. Auch an die Normdichte sind relativ hohe Anforderungen zu stellen. Das Gesetz muss insbesondere betreffend verwendete Daten, Zweck und Voraussetzungen sowie Art und Weise des Profilings so klar und deutlich formuliert sein muss, dass der damit einhergehende Eingriff in die Grundrechte der betroffenen Personen für diese vorhersehbar ist

[29] Zur Bearbeitung durch Cloud-Service-Provider (insbesondere Cloud-Service-Provider) vgl. Ziff. 2.5. unten.

1.1.3 «Daten juristischer Personen»

Unter dem bisher geltenden Datenschutzrecht fielen auch die Daten juristischer Personen unter den Begriff Personendaten. Mit dem nDSG fallen diese Daten nicht mehr in den Anwendungsbereich des Gesetzes.

Die nötigen Rechtsgrundlagen für den Umgang mit Daten juristischer Personen wurden mit der Revision des DSG vom September 2020 im Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR 172.010) eingefügt (Art. 57r ff. nRVOG). Diese Bestimmungen lehnen sich punktuell an das nDSG an[30].

Daten juristischer Personen dürfen *bearbeitet* werden, soweit dies für die Erfüllung der Aufgaben einer Verwaltungseinheit notwendig ist und diese Aufgaben in einem Gesetz im formellen Sinn umschrieben sind (Art. 57r Abs. 1 nRVOG). Dies gilt auch für besonders schützenswerte Daten von juristischen Personen. Sind diese Anforderungen erfüllt, so ist grundsätzlich keine weitere spezialgesetzliche Grundlage mehr nötig, ausser die Datenbearbeitung führt zu einem sehr schwerwiegenden Eingriff in die Grundrechte der betroffenen juristischen Person.

Artikel 57r Absatz 2 nRVOG definiert besonders schützenswerte Daten juristischer Personen:

- Daten über verwaltungs- und strafrechtliche Sanktionen;
- Daten über Berufs-, Geschäfts- und Fabrikationsgeheimnisse.

Für die *Bekanntgabe* von Daten juristischer Personen gelten indessen strengere Vorgaben. Diese muss in einer spezialgesetzlichen Grundlage vorgesehen sein (Art. 57s Abs. 1 nRVOG). Für gewöhnliche Daten genügt in der Regel eine Verordnungsbestimmung; bei besonders schützenswerten Daten ist dagegen grundsätzlich eine Grundlage in einem Gesetz im formellen Sinn erforderlich[31].
Diese Vorgabe wäre für Cloud-Lösungen somit beispielsweise dann zu beachten, wenn Daten über Berufs-, Geschäfts- und Fabrikationsgeheimnisse bearbeitet werden. Für die Bekanntgabe solcher Daten müssten zudem weitere Schutzmassnahmen getroffen werden. Sie müssten pseudonymisiert oder zumindest für die Phase «data in transit» und «data at rest» (vgl. Teil 2, Ziff. 1.2.2) angemessen verschlüsselt werden. Für die Phase «data in use» sind ebenfalls angemessene Schutzmassnahmen (z.B. beschränkter Zugriff oder geschützte Datenbearbeitung[32]) zu prüfen.[33]

1.2 Technische Ansätze zum Schutz der Daten

Es gibt verschiedene Ansätze, um Daten vor unbefugtem Zugriff bzw. unbefugter Kenntnisnahme zu schützen. Im Cloud-Kontext stehen die Entpersonalisierung (Anonymisierung und Pseudonymisierung), Tokenisierung und (mit gewissen Einschränkungen) die Verschlüsselung von Daten im Zentrum.

1.2.1 Anonymisierung und Pseudonymisierung von Daten

Anonymisierung bedeutet, dass Daten endgültig von ihrem Personenbezug befreit werden. Eine Umkehrbarkeit muss ausgeschlossen sein. Eine Anonymisierung ist daher wohl nur eine Option, wenn die Daten nicht länger personenbezogen verwendet werden müssen, so z.B. für statistische Anwendungen. Ihre Bearbeitung fällt danach auch nicht mehr unter das Datenschutzgesetz. Eine vollständige Anonymisierung zu erreichen kann technisch anspruchsvoll sein, da mit Analytics-Methoden Dritte auch bei vordergründig anonymen Daten unter Umständen einen Personenbezug wiederherstellen können.[34] Entsprechend kann eine vollständige Anonymisierung derart tiefgreifende Eingriffe in die Daten erfordern, dass diese ihren Verwendungszweck nicht mehr erfüllen können.

Pseudonymisierung von Daten bedeutet, dass der Personenbezug bestehen bleibt, dieser aber für Dritte nicht erkennbar ist. In der Regel bedeutet dies, das einzelne Elemente von Datensätzen durch

[30] Vgl. BJ, Totalrevision des Datenschutzgesetzes (DSG). Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Verwaltungseinheite, Ziff. 3.2 (Entwurf).
[31] Unter gewissen Voraussetzungen kann auch eine Verordnung genügen, nämlich wenn die Datenbekanntgabe für eine formellgesetzlich geregelte Aufgabe unentbehrlich ist und der Bearbeitungszweck für die Grundrechte der betroffenen juristischen Person keine besonderen Risiken mit sich bringt (BJ, Totalrevision DSG, Ziff. 3.2.3). Allerdings wird eine Cloud-Lösung und die damit verbundene Bekanntgabe in der Regel kaum «unentbehrlich» sein. Die in Art. 57s weiter vorgesehenen Ausnahmen und Spezialfälle betreffen Bekanntgaben im Einzelfall und können für Cloud-Lösungen kaum Anwendung finden.
[32] Z.B. «Confidential Computing», bei dem sensible Daten während der Verarbeitung in geschützten Prozessoren isoliert werden; vgl. z.B. https://www.ibm.com/cloud/learn/confidential-computing.
[33] Es ist offensichtlich vergessen worden, Art. 9 nDSG für die Daten juristischer Personen ins RVOG zu überführen. U.E. greift aber (i.S. einer echten Lücke) trotzdem die Privilegierung der Bekanntgabe an Auftragsbearbeiter gemäss Art. 9 nDSG. Eine Verschärfung gegenüber dem heutigen Regelungsgehalt war ganz offensichtlich nicht die Absicht. Somit ist für die Nutzung einer Cloud-Lösung an sich keine gesetzliche Grundlage erforderlich.
[34] Vgl. dazu GA WIDMER, S. 9f.s

Platzhalter ersetzt werden, z.B. Namen durch Nummern (ähnlich auch das Verfahren der «Tokenisierung»[35]). Das verantwortliche Organ verfügt über den entsprechenden Schlüssel. Eine Pseudonymisierung bedeutet aber in der Regel nur, dass es für Dritte erschwert wird, wieder einen Personenbezug herzustellen. Wenn Dritte über kontextbezogene Daten oder Informationen verfügen, ist eine Zuordnung der Daten zu den betreffenden Personen unter Umständen möglich. Eine Pseudonymisierung ist dann ausreichend, wenn aufgrund der Umstände das Risiko gering erscheint, dass Dritte, welche nicht über die entsprechenden Schlüssel verfügen, in der Lage sind, mit einem vernünftigerweise erwartbaren Aufwand[36] die Daten wieder Personen zuzuordnen. In diesem Fall finden die Bestimmungen des nDSG gegenüber Dritten keine Anwendung.[37]

In rechtlicher Hinsicht haben die Anonymisierung oder Pseudonymisierung zur Folge, dass nicht auf den Klartext zugegriffen werden kann und damit keine Datenbekanntgabe an Dritte erfolgt (weil es eben keine Personendaten mehr sind, da vom Cloud-Service-Provider kein Rückschluss auf eine konkrete Person mehr gezogen werden kann).

Bei der Tokenisierung handelt sich um einen Prozess, bei dem ein aussagekräftiger Teil der Daten in eine zufällige Zeichenfolge, ein so genanntes Token, umgewandelt wird. Ein Token hat keinen sinnvollen Wert und dient nur als Ersatz für die eigentlichen Daten. Dieses Token wird dann z.B. in einer Cloud-Datenbank gespeichert. Tokens können in keiner Art und Weise verwendet werden, um zu den ursprünglichen Daten zu gelangen. Das liegt daran, dass bei der Tokenisierung im Gegensatz zur Verschlüsselung keine kryptografische Methode zur Umwandlung von Daten in die verschlüsselte Form (Chiffrat) verwendet wird. Die Tokenisierung wird insbesondere bei sicheren Zahlungssystemen verwendet.

1.2.2 Verschlüsselung

Bei der *Verschlüsselung*[38] werden die Daten so verändert, dass der Personenbezug – bzw. der Informationsgehalt der Daten allgemein – für Dritte, die nicht über einen Schlüssel verfügen, nicht sichtbar ist. Solange die Verschlüsselung verlässlich bzw. hinreichend stark ist und die Schlüssel geheim sind, kann nur der Inhaber der Schlüssel die Daten wiederherstellen.

Der Nutzen der Verschlüsselung als Massnahme zur Gewährleistung von Datenschutz und -sicherheit ist je nach Phase des Bearbeitungsprozesses und je nach Verschlüsselungsstandard unterschiedlich. Kritisch ist dabei das Schlüsselmanagement[39] , welches hohes Gewähr dafür bietet, dass die mit der Verschlüsselung verfolgten Ziele erreicht werden können. Dabei ist zu klären, wer den Schlüssel tatsächlich verwaltet, ob der Schlüssel aufgeteilt wird (eine Person kennt nur die Hälfte des Schlüssels oder verfügt über einen zweiten Schlüssel → Double Key Encryption) und wie ein Verlust des Schlüssels verhindert wird oder Schlüssel wiederhergestellt werden können (Key Recovery). Andernfalls könnten Daten unwiderruflich verloren gehen. Ebenfalls ist zu beachten, dass die Technologie zur Verschlüsselung einem raschen Wandel unterliegt und die Verschlüsselung gegebenenfalls der neuen Technologie angepasst werden muss. Für das Schlüsselmanagement bestehen unterschiedliche Ansätze. Grundsätzlich sind Lösungen anzustreben, bei denen die Auftragsdatenbearbeitenden (Cloud-Service-Provider, Cloud-Hoster, weitere Dienstleistende; vgl. Teil 2, Ziff. 1.2.2) keinen oder nur sehr eingeschränkten Zugriff auf die Schlüssel haben (z.B. «Bring Your own Key» unter Einsatz eines dezidierten Hardware Security Moduls in der Cloud oder «Keep your own Key»)[40]. Das gilt auch für andere Ansätze, die dazu dienen, Daten vor unberechtigten Kenntnisnahme zu schützen, wie beispielsweise durch Beschränkung der Zugriffsrechte und durch ergänzende Sicherheits- bzw. Authentifizierungssysteme (vgl. Anhang C).

Die Technologien zur Verschlüsselung entwickeln sich ständig weiter, daher ist darauf zu achten, dass eine gewählte Verschlüsselungslösung stets dem aktuellen Stand der Technik entspricht. Zu beachten ist auch der Zeithorizont, da heute sichere Verschlüsselungstechniken in der Zukunft unsicher werden können. Die Methoden der Verschlüsselung variieren je nach Zustand der Daten. Im Zusammenhang mit der Verschlüsselung ist jeweils insbesondere zu prüfen, ob die verwendeten Verschlüsselungs-

[35] Vgl. MILLARD, S. 38.
[36] Wie hoch der Aufwand ist, von dem anzunehmen ist, dass ein Angreifer ihn vernünftigerweise betreiben würde, ist immer im konkreten Fall im Rahmen der Risikobeurteilung zu prüfen und ist jeweils von verschiedenen Faktoren abhängig (insbesondere welche anderen Daten für eine Re-Identifizierung zur Verfügung stehen). Die Beurteilung kann sich aufgrund der technischen Entwicklung ändern.
[37] Vgl. dazu GA WIDMER, S. 10.
[38] Vgl. zur Verschlüsselung auch NCSC, Nutzbarkeit von Cloud-basierten Dienstangeboten in der Bundesverwaltung, 8.11.2021.
[39] Für eine Übersicht vgl. NCSC, a.a.O., S. 3.
[40] Im Rahmen der Ausschreibung WTO 20007 musste eine entsprechende Anforderung zugesichert werden; vgl. Anforderungskatalog, S. 8 (TS03); vgl. auch DAVID ROSENTHAL, Schweizer Banken in die Cloud; Zu den verschiedenen Ansätzen des Schlüsselmanagements vgl. NCSC, a.a.O., S. 3.

standards sowie die Massnahmen zum Schutz der Schlüssel genügend sind[41].Verschlüsselungslösungen, insbesondere Key Management Architekturen können unterschiedlich ausgestaltet und in verschiedenen Stadien der Datenbearbeitung implementiert sein, je nachdem, ob die Daten von einem Rechner zum anderen transportiert werden (*data in transit*), bearbeitet werden (*data in use*) oder auf einer Cloud Umgebung gespeichert werden (*data at rest*).

Data in transit

Es gibt diverse Technologien zum Schutz der Übertragung der Daten. Daten können in verschlüsselter Form oder mittels einer sicheren Datenverwaltung übertragen werden (beispielsweise über SFTP, HTTPS mittels TLS oder VPN). Mit SCION gibt es eine weitere und neue Schweizer Technologie, die eine sichere Datenübertragung (Routing) automatisiert gewährleisten soll.[42] Neben der Verschlüsselung können CASB (Cloud Access Security Brokers) einen weiteren Schutz bieten. Bei CASB handelt es sich um Sicherheitssysteme, welche die Einhaltung von Sicherheitsvorgaben automatisiert überprüfen und Daten allenfalls für bestimmte Nutzer sperren können, wenn diese die vorgegebenen Sicherheitsstandards nicht einhalten. Auch Gateways, die die Verschlüsselung oder Pseudonymisierung bzw. Tokenisierung automatisieren, können als Schutzmassnahme eingesetzt werden[43].

Data at rest

Die Daten werden weder bearbeitet, noch wird auf sie zugegriffen. Sie ruhen an einem Ort (beispielsweise auf einem Datenserver). In diesem Zustand ist es relativ einfach die Daten zu schützen. Sie können verschlüsselt werden, sei es auf Ebene Disk, Dateien oder ganzer Datenbanken. Ebenfalls gibt es die Möglichkeit die Daten durch CASB zu schützen. Sobald die Daten jedoch die Cloud verlassen, kann der Schutz durch CASB nicht mehr gewährleistet werden. Wenn der Schlüssel beim Cloud-Service oder – Hosting Cloud-Service-Provider liegt (je nach Art des Schlüsselmanagements), kann ein Zugriff nicht vollkommen ausgeschlossen werden.

Data in use

Es handelt sich hierbei um Daten in Verwendung, das heisst eine Anwendung zur Bearbeitung der Daten. In diesem Zustand sind die Daten am anfälligsten, weil sie zur Bearbeitung entschlüsselt werden müssen und sich zu diesem Zeitpunkt im Arbeitsspeicher befinden. Auch hier gibt es Möglichkeiten die Daten vor unbefugten Zugriff zu schützen. Zum einen durch Identitätsmanagement-Tools und zum anderen durch Information Rights Management (IRM). Durch Identitätsmanagement-Tools wird der Kreis der zur Bearbeitung Berechtigten eingeschränkt und kontrolliert. Durch IRM werden die Bearbeitungen, die der Bearbeiter mit den Daten vornehmen kann, eingeschränkt. Sie können dann beispielsweise nicht gedruckt oder verändert werden. Der Einsatz von vertrauenswürdiger Hardware ist eine weitere mögliche Schutzmassnahme (Trusted Execution Environment TEE oder «Secure Enclave»)[44]. Eine neue Technik ist das Confidential Computing, dass es den Cloud-Service-Providern verunmöglicht auf Daten während der Bearbeitung zuzugreifen.[45]

Nach heutigem Stand der Technik ist das Risiko des Datenzugriffs durch Unbefugte bei *data in use* in der Regel am ehesten gegeben[46]. Durch eine Kombination der verschiedenen Schutzmassnahmen kann das Risiko indessen reduziert werden. Die Risikoanalyse muss im Einzelfall aufzeigen, welche Schutzmassnahmen für die jeweiligen Daten am angemessensten sind und ob die möglichen Massnahmen insgesamt ausreichen, um einen adäquaten und rechtskonformen Schutz zu erreichen (siehe Anhänge C bis E).

[41] Unter Umständen sind sogar Szenarien denkbar, bei denen eine durchgehende Verschlüsselung dazu führen könnte, dass gar keine Datenbekanntgabe stattfindet, z.B. beim blossen Hosting von Daten in der Cloud.
[42] Nur Gateway to Gateway, Broad Network Access ist zur Zeit nicht unterstützt, da Endgeräte nicht z.B. mittels eines SCION Agents unterstützt werden. Weiterführende Informationen zu SCION: SCION Internet Architecture (scion-architecture.net).
[43] Auch neue Ansätze wie Secure Access Service Edge (SASE) können eingesetzt werden, inkl. Zero Trust Network Access (ZTNA) .Vgl. auch MILLARD, S. 38.
[44] Vgl. NCSC, a.a.O., S. 3; MILLARD, Cloud Computing Law, S. 39 f.
[45] Vgl. NCSC. Technologiebetrachtung «Confidential Coputing.
[46] Soweit Data at rest und in transit verschlüsselt sind und der CSP nicht ohne Weiteres Zugriff auf die Schlüssel hat.

1.3 Datensicherheit

1.3.1 Grundsätze

Artikel 8 nDSG verankert die Pflicht für Verantwortliche und Auftragsbearbeiter durch geeignete dem aktuellen Stand der Technik entsprechende Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten. Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

Der Entwurf der Verordnung zum Datenschutzgesetz gibt Grundsätze vor betreffend[47]:

- Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität);
- zu berücksichtigende Risiken (insbesondere zufällige oder unbefugte Vernichtung, zufälliger Verlust, technische Fehler, Fälschung, Diebstahl und widerrechtliche Verwendung sowie unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen);
- Kriterien, nach welchen die zu ergreifenden Massnahmen zu bemessen sind (Zweck der Datenbearbeitung, Art und Umfang der betroffenen Daten und der vorgesehenen Datenbearbeitung, mögliche Risiken für die betroffenen Personen, gegenwärtiger Stand der Technik).

Weitere Vorgaben zur Datensicherheit finden sich auch in weiteren rechtlichen Vorgaben (vgl. Teil 2, 0 und 4.2 insbesondere Cyberrisikenverordnung (CyRV)[48], Informationssicherheitsgesetz (ISG)[49] und die noch bis zum Inkrafttreten des ISG geltende Informationsschutzverordnung (IschV). Auch einige Weisungen regeln Sicherheitsaspekte, etwa beim Einsatz von Mobilgeräten oder zum IT-Grundschutz[50].

Findet entgegen allen Massnahmen eine Verletzung der Datensicherheit statt, so sieht Artikel 24 nDSG zudem eine Meldepflicht vor, welche ausdrücklich auch Auftragsbearbeiter trifft.

1.3.2 Bearbeitungsreglement

Die Massnahmen sind in einem Bearbeitungsreglement[51] (Art. 5 i.V.m. Art. 6 Abs. 2 E-DSVE-DSV) detailliert zu regeln. Dieses Bearbeitungsreglement ist dann zu erstellen, wenn die Voraussetzungen von Artikel 6 Absatz 1 E-DSV erfüllt sind. Die für die Public-Cloud-Nutzung zur Verfügung stehenden technischen Massnahmen werden in der Regel durch den jeweiligen Cloud-Service Anbieter festgelegt. Die eingesetzten Mechanismen können manchmal aus einem Service-Katalog ausgewählt werden (davon sind die Lizenzen und die Kosten abhängig). Sie müssen aber auch dokumentiert werden (vgl. auch Anhang C). In einem Bearbeitungsreglement sind dabei primär die organisatorischen Massnahmen zu definieren, also insbesondere wer welche Daten wie (und ggf. wann und wie häufig) bearbeiten darf. Welche technischen Massnahmen hinreichenden Schutz bieten ist auch nach dem aktuellen Stand der Technik zu beurteilen und kann sich daher mit dem Zeitablauf ändern.

Für Cloud-Lösungen sind die folgenden wichtigsten Risiken mit Blick auf die Datensicherheit zu nennen, die durch technische und organisatorische Massnahmen angemessen zu adressieren und für die – soweit möglich – entsprechende vertragliche Regelungen[52] vorzusehen sind (einschliesslich Haftungsregelungen bzw. Konventionalstrafen; vgl. zum Ganzen auch Anhang C)[53]:

- Unklare Regelung von Compliance-Anforderungen und unklarer Umgang mit Sicherheitsvorfällen (insbesondere Meldung von sicherheitsrelevanten Vorkommnissen): Die Compliance-Anforderungen (insbesondere Erfüllung von Zertifizierungen, Offenlegungen von Auditergebnissen) sind vertraglich festzulegen; entsprechende Kontrollen sind durchzuführen. Ebenso die Pflicht zur Meldung von sicherheits- und datenschutzrelevanten Vorkommnissen (siehe auch Art. 24 nDSG).[54]

---

[47] Vgl. auch den entsprechenden Leitfaden des EDÖB: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/TOM.pdf.download.pdf/guideTOM_de_2015.pdf ; sowie GA WIDMER, S. 15.
[48] Die Cyberrisikenverordnung wird mit dem ISG und ISV aufgehoben und in diese integriert.
[49] Es tritt voraussichtlich Mitte 2023 in Kraft.
[50] NCSC, Si001 IT-Grundschutz in der Bundesverwaltung vom 1.3.2022 (https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz_V5-0-d.pdf.download.pdf/Si001-IT-Grundschutz_V5-0-d.pdf); E026 Einsatzrichtlinie Arbeitsplatzsystem, insbes. 2.3 – 2.5.
[51] Vgl. https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2014/06/was_muss_in_einembearbeitungsreglementaufgefuehrtwerden.pdf.download.pdf/was_muss_in_einembearbeitungsreglementaufgefuehrtwerden.pdf
[52] Für Cloud-Dienstleistungen, die unter WTO 20007 beschafft wurden, geben die mit den Dienstleistern abgeschlossenen Rahmenverträge grundsätzlich vor, welche technischen Massnahmen zur Verfügung stehen. Allenfalls können in beschränktem Ausmass weitere Massnahmen vereinbart werden.
[53] Vgl. auch Anhang C.
[54] In der Ausschreibung zur WTO 20007 wurde dieser Aspekt in Ziff. 8.1 bereits definiert.

- Unklare organisatorische Regelungen im Umfeld der Shared Responsibility: Klare AKV müssen vereinbart werden, auch im Umfeld der Cloud Security (z.B. Interaktionen mit dem CSP SOC).
- Bearbeitung von Daten auf gemeinsam mit «fremden» Dienstleistungsbeziehenden genutzten Infrastrukturen und dadurch insbesondere erhöhtem Risiko eines Versagens der Datenisolation bei einer bloss logischen statt physischen Trennung: Physisch getrennte Infrastrukturen vereinbaren; besondere Architekturmodelle.
- Klärung der Möglichkeiten zur Verschlüsselung von Daten. Welche Arten der Verschlüsselung gibt es? Können data in transit und data at rest angemessen verschlüsselt werden? Wo liegen die Schlüssel? Wer hat Zugang zu den Schlüsseln?
- Fehlende Verfügbarkeit, z.B. aufgrund mangelnder Netzwerkkapazitäten, wegen Mängeln bei der Zusammenarbeit zwischen Cloud-Service-Provider, Cloud-Exchange Provider und Cloud-Nutzer oder wegen mangelnden Schutzes beim Cloud-Service-Provider gegen Naturereignisse, Strommangellagen o.ä.: vertragliche Regelung und ggf. Kontrollen vor Ort.
- Ausspähen von Informationen mittels kompromittierter Hardware: Wieviel grösser (oder sogar kleiner) dieses Risiko im Vergleich zu «On-Premise» Lösungen ist, ist schwierig einzuschätzen, denn es besteht in gewissem Ausmass auch beim Bearbeiten mit eigener Hardware.

Daraus abgeleitet sind weitere sicherheitsrelevante Risiken identifizierbar und zu klären:

- Abhängigkeiten vom Anbieter, erschwerte Datenmigration bzw. beschränkte Datenportabilität, insbesondere im Fall der Beendigung der Zusammenarbeit: Vertragliche Garantien verlangen (Schnittstellen, Zusicherung von Ressourcen unter Absicherung durch Konventionalstrafen).
- Mangel an erforderlichen personellen Ressourcen mit adäquatem Fachwissen (insbesondere beim Auftraggeber): Vertragliche Garantien verlangen.
- Sicherheitsrisiken aufgrund von böswilligen Mitarbeitenden beim Cloud-Service-Provider oder von ihm beauftragten Unterauftragnehmer (Insider-Angriffe): Zugriffsbeschränkungen, je nach betroffenen Daten: Vertragliche Vereinbarung von Sicherheitsprüfungen gemäss den Standards in der Bundesverwaltung.

1.4 Vor der Nutzung eines Cloud-Services: Allfällige Datenschutz-Folgenabschätzung

Gemäss Artikel 22 Absatz 1 nDSG muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Mit diesem Instrument sollen Risiken frühzeitig erkannt und allfällige Schutzmassnahmen getroffen werden. Als hohes Risiko nennt Artikel 22 Absatz 2 nDSG beispielsweise die umfangreiche Bearbeitung von besonders schützenswerten Personendaten. In der Datenschutz-Folgenabschätzung müssen die geplante Datenbearbeitung, deren Risiken für die Persönlichkeit oder die Grundrechte sowie die bereits getroffenen oder noch zu treffenden Schutzmassnahmen beschrieben werden (Art. 22 Abs. 3 nDSG). Bleibt trotz der getroffenen oder geplanten Massnahmen ein hohes «Restrisiko» für die Persönlichkeit oder die Grundrechte der betroffenen Person bestehen, muss der EDÖB konsultiert werden (Art. 23 Abs. 1 nDSG).

In Bezug auf Cloud-Projekte bedeutet dies, dass mittels der Datenschutz-Folgenabschätzung die potenziellen Risiken in Bezug auf den Datenschutz eruiert werden müssen (vgl. auch Anhang D), bevor Daten in die Cloud ausgelagert werden können, die potentiell Rückschlüsse auf Personen zulassen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Wie die Datenschutz-Folgeabschätzung durchzuführen ist und ob sie in bestehende Instrumente (z.B. die Schutzbedarfsanalyse) integriert werden kann, wird derzeit geprüft und die Praxis zeigen.

1.5 Findet mit der Nutzung eines Cloud-Services eine Datenbearbeitung durch einen Auftragsbearbeiter statt?

1.5.1 Auftragsdatenbearbeitung im nDSG

Artikel 9 nDSG regelt die Datenbearbeitung durch Auftragsbearbeiter. Die Bearbeitung von Personendaten kann durch die Gesetzgebung oder vertraglich einem Auftragsbearbeiter übertragen werden,

wenn dieser die Daten nur im Umfang und zum Zweck bearbeitet, wie der Verantwortliche selbst es tun dürfte[55]. Der Auftragsbearbeiter darf insbesondere Daten nicht zu eigenen Zwecken bearbeiten.[56]

Verantwortlich bleibt die Verwaltungseinheit, da sie – im Rahmen der gesetzlichen Grundlage für die Bearbeitung – entscheidet, wie bzw. mit welchen Mitteln die Daten bearbeitet werden (Art. 9 Abs. 2 nDSG). Sie muss die Auftragsdatenbearbeiter sorgfältig auswählen, instruieren und (soweit möglich bzw. vertraglich vorgesehen) kontrollieren und damit aktiv sicherstellen, dass diese die datenschutzrechtlichen Vorgaben so einhalten, wie sie es selbst tun müssten.

Eine Bundesstelle als für die Datenbearbeitung Verantwortliche, muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Sie hat also eine Gewährleistungspflicht. Diese Gewährleistung kann nur umgesetzt werden, wenn regelmässige Kontrollen erfolgen, z.B. durch Auditierung.

Das Gesetz sieht zudem ausdrücklich vor, dass der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger schriftlicher Genehmigung der verantwortlichen Bundesstelle einem Dritten übertragen darf (Art. 9 Abs. 3 nDSG). Diese kann auch vorgängig beispielsweise im Vertrag mit dem Cloud-Service-Provider erteilt werden. In diesem Fall sollte der Bundesstelle ein Widerspruchsrecht eingeräumt werden, mit dem sie solche Unterauftragsbeziehungen ablehnen kann. Solche Unterauftragsbearbeiter werden durch Cloud-Service-Provider häufig eingesetzt (z.B. für das physische Hosting der Daten, für Netzwerkdienstleistungen und/oder für Unterhalt und Wartung; vgl. unten Ziff. 1.5.3).

Zusätzlich zum Datenschutzgesetz regelt Artikel 11 der Verordnung über die digitale Transformation und die Informatik (VDTI; 172.010.58) das Zugänglichmachen von Daten für externe Leistungserbringer[57]. Daten, die nicht allgemein zugänglich sind, dürfen externen Leistungserbringern nur zugänglich gemacht werden, wenn die folgenden Voraussetzungen erfüllt sind:

- Das Zugänglichmachen der Daten ist zur Erbringung der Leistung *erforderlich*. D.h., die Daten müssen für den Leistungserbringer zwingend verfügbar sein, damit er seinen Auftrag erfüllen kann bzw. es würde einen nicht verhältnismässigen Aufwand bedeuten, wenn er dies ohne Zugang zu den Daten (bzw. nur in entpersonalisierter oder verschlüsselter Form) tun müsste.
- Die für die Daten verantwortliche Behörde hat schriftlich zugestimmt. Macht die für die Daten verantwortliche Behörde die Daten selber zugänglich (und nicht etwa ihr bundesinterner Leistungserbringer), so ist für die Zustimmung nach Absatz 1 Buchstabe b ihre vorgesetzte Stelle zuständig.
- Es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern.

1.5.2 Auftragsdatenbearbeitung im Cloud-Kontext

Der Cloud-Service-Anbieter ist nicht in jedem Fall zwingend auch Auftragsdatenbearbeiter. Die entsprechende Qualifikation hängt insbesondere auch vom gewählten Modell ab (z.B. SaaS, vgl. oben Teil 1 Ziff. 2.1).

Wie weit eine Auftragsdatenbearbeitung der in die Cloud übermittelten Daten durch den CSP (Cloud Service Provider) überhaupt stattfindet, ist im Einzelfall abzuklären. In der Regel wird er, wenn überhaupt, auf Daten im Klartext nur in ganz bestimmten und im Voraus vereinbarten Einzelfällen zugreifen und diese selbst bearbeiten dürfen. Ausnahme davon bildet der Zugriff insbesondere auf Randdaten; solche werden vom CSP in der Regel zumindest für die Abrechnung seiner Dienstleistung erhoben und bearbeitet.

1.5.3 Beizug von Unterauftragnehmern durch den Cloud-Service-Provider

Für die Erfüllung seiner Aufgaben wird der Cloud-Service-Provider regelmässig auf Unterauftragnehmer zurückgreifen. Diese nehmen oft Kernfunktionen wahr, sei es beim physischen Hosting der Daten

[55] Vgl. zum geltenden Artikel 10a DSG z.B. BAERISWYL in: ders. / Pärli, Datenschutzgesetz (DSG), Bern 2015, Art. 10a, N 14 ff.).
[56] Standardverträge von Cloud-Service-Providern können vorsehen, dass solche Bearbeitungen zu eigenen Zwecken vorgenommen werden können. Diesfalls müsste eine solche Bearbeitung vertraglich ausgeschlossen werden, vgl. ROSENTHAL, Schweizer Banken in die Cloud, Oft erfolgen solche Bearbeitungen zu eigenen Zwecken des Auftragsbearbeiters lediglich auf Basis von vorher anonymisierten oder pseudonymisierten Daten, und sie dienen letztlich im Rahmen der Verbesserung der Service-Sicherheit oder -qualität doch wieder den Zwecken des Auftraggebers. In diesem Fall ist genau zu beschreiben, wieweit z.B. eine Auswertung der übermittelten personenbezogenen Daten für die Bereitstellung der Cloud-Dienste erforderlich und zulässig ist.
[57] Hier geht es nicht eigentlich um den Daten- sondern um den Geheimnisschutz, vgl. unten Ziff. 2.2.

(Cloud Hosting Cloud-Service-Provider), bei der Datenübermittlung (Betreiber von Netzwerken) oder im Bereich der Wartung oder Behebung von Störungen (Support). Dabei kann es erforderlich sein, dass die Unterauftragnehmer Zugriff auf unverschlüsselte Daten haben müssen, um den Support überhaupt gewähren zu können. Aus diesem Grund ist sicherzustellen, dass Dritte, die als Unterauftragnehmer dem Cloud-Service-Provider unterstellt sind, an die gleichen Regelungen gebunden sind, wie der Cloud-Service-Provider selbst (vgl. Art. 9 nDSG und 11 VDTI). Dies muss zwingend vertraglich so festgehalten werden. Gegebenenfalls sind zusätzliche Massnahmen nötig.

1.6 Datenbekanntgabe ins Ausland

1.6.1 Grundsätze

Artikel 16 ff. nDSG regeln die Bekanntgabe von Personendaten ins Ausland. Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 nDSG)[58]. Diese Staaten werden in einer Liste im Anhang der E-DSV aufgeführt. Aktuell erfüllen namentlich die Mitgliedstaaten der EU, UK, Argentinien und Neuseeland diese Anforderungen, im Gegensatz zu den USA und China.

Weiter dürfen Daten in gewissen Ausnahmefällen in Staaten übermittelt werden, die nicht über ein angemessenes Datenschutzniveau verfügen, insbesondere wenn die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat (Art. 17 Abs. 1 Bst. a nDSG). Indessen ist darauf hinzuweisen, dass Einwilligungslösungen für systematische Datenbearbeitungen aufgrund der hohen entsprechenden Anforderungen (vgl. Art. 6 Abs. 6 und 7 nDSG) keine geeignete Lösung sind.

Ist ausnahmsweise eine Datenbearbeitung in einem Staat erforderlich, der nicht über eine angemessene Datenschutzgesetzgebung verfügt, so ist eine entsprechende vertragliche Absicherung vorzusehen, etwa unter Verwendung der vom EDÖB genehmigten bzw. bereitgestellten Standardvertragsklauseln[59] oder spezifischer Garantien, die die zuständige Verwaltungseinheit erarbeitet und dem EDÖB vorgängig mitgeteilt hat[60]. Zudem sind auch angemessene technische und organisatorische Massnahmen zu treffen, z.B. namentlich eine Verschlüsselung der Daten, welche den Zugriff auf den personenbezogenen Dateninhalt durch den (ausländischen) Auftragsdatenbearbeiter und allfällige Unterauftragnehmer weitgehend ausschliesst[61]. Allenfalls ist zu prüfen, ob Vorgaben für «data in transit» möglich sind, z.B. betreffend das Routing[62] (vgl. Teil 2, Ziff. 1.2.2).

Weiter zu berücksichtigen ist in solchen Fällen bei der Beschaffung der Personendaten die besondere Informationspflicht nach Art. 19 Abs. 4 nDSG greifen kann, wenn Daten ins Ausland bekannt gegeben werden und im Empfangsstaat keine angemessene Datenschutzgesetzgebung besteht. Soweit die Bearbeitung nicht gesetzlich vorgesehen ist (Art. 20 Abs. 1 Bst. b nDSG; was allerdings für Behörden ohnehin eine allgemeine Voraussetzung ist) müssen die Betroffenen über den Empfangsstaat und ggf. die Garantien nach Art. 16 Abs. 2 nDSG informiert werden. Ausnahme davon bilden Artikel 20 Absatz 2 nDSG, nämlich wenn die Information nicht möglich ist oder die Information einen unverhältnismässigen Aufwand erfordert.

1.6.2 Im Cloud-Kontext

Ob bei Cloud-Sourcings eine Datenbekanntgabe im Sinne des DSG vorliegt, ist im Einzelfall zu prüfen[63]. Dies ist z.B. dann grundsätzlich nicht der Fall, wenn Daten pseudonymisiert oder tokenisiert sind (vgl. oben Ziff. 1.2.2) oder wenn andere Vorkehrungen getroffen werden, um eine Kenntnisnahme vom Dateninhalt bzw. «Klartext» durch den CSP auszuschliessen.

---

[58] Die Veröffentlichung von Personendaten in elektronischer Form mittels automatisierter Informations- und Kommunikationsdienste beispielsweise auf Webseiten der Bundesverwaltung, die auch aus dem Ausland abgerufen werden könnten gilt nicht als Bekanntgabe ins Ausland (Art. 18 nDSG).

[59] Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland (admin.ch). Im Rahmen der Ausschreibung WTO 20007 war eine entsprechende Anforderung vorgesehen; vgl. Anforderungskatalog, S. 12 (ZK03)

[60] Vgl. dazu die Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug vom Juni 2021 des EDÖB (Startseite > Datenschutz > Handel und Wirtschaft > Übermittlung ins Ausland).

[61] Es könnte allenfalls die Frage gestellt werden, ob überhaupt von einer «Bekanntgabe» auszugehen ist, wenn der CSP die Daten selbst gar nicht bearbeiten soll bzw. darf und sein Zugriff darauf weitgehend ausgeschlossen werden kann.

[62] So ist etwa eine Verpflichtung zur Nutzung des SCION-Standards denkbar.

[63] Vgl. dazu auch z.B. BAERISWYL in: ders. / Pärli, Datenschutzgesetz (DSG), Bern 2015, Art. 10a, N 43.

Die Cloud-Service-Provider sind vertraglich dazu zu verpflichten, sich generell an das schweizerische Recht und insbesondere an die datenschutzrechtlichen Vorgaben zu halten, als Gerichtsstand ist grundsätzlich die Schweiz zu vereinbaren[64].

Bei der Nutzung von Cloud-Lösungen muss sich der Cloud-Service-Provider gegenüber dem Cloud-Nutzer verpflichten, dass Daten nur in dem vom Cloud-Nutzer bestimmten ausländischen Staat oder in bestimmten ausländischen Staaten bearbeitet und gespeichert werden[65]. Es muss vom Cloud-Service-Provider offengelegt werden, wo der Cloud-Service effektiv betrieben wird (inkl. Supportleistungen), wer von wo aus auf die Daten Zugriff hat; dies ist vertraglich festzuhalten (vgl. Anhang C, D). Eine Datenbearbeitung an einem ungewissen Ort ist nicht akzeptabel.

1.7 Behördenzugriffe im Ausland

Befinden sich Daten des Bundes im Ausland, so ist es möglich, dass Daten von ausländischen Behörden bei Dienstleistern herausverlangt werden können (statt beim Bund als Datenherrn auf dem Weg der Rechtshilfe). Dabei können grob drei Szenarien von möglichen Behördenzugriffen (und entsprechende Rechtsgrundlagen) unterschieden werden:

- Justizverfahren,
- Nationale Sicherheit bzw. präventive Kriminalitätsbekämpfung (insbesondere Terrorismus) und
- nachrichtendienstliche Auslandüberwachung[66].

In allen drei Fällen kann sich die Situation ergeben, dass auf Daten des Bundes nach rechtmässig ausländischem Recht, aber in Verletzung von Schweizer Recht und von vertraglichen Vereinbarungen mit den Dienstleistern, durch ausländische Behörden zugegriffen wird[67]. Diesbezüglich ist die Frage zu stellen, ob die Rechtsordnung in einem Zielland besondere Risiken beinhaltet, etwa, weil die verfahrensmässigen Sicherungen ungenügend sind bzw. die Durchsetzung von Ansprüchen als besonders schwierig beurteilt wird.

Ganz allgemein bestehen im Völkerrecht für den Zugriff ausländischer Staaten auf Behördendaten eines anderen Staates aus dem Bereich der Staatenimmunität Ansatzpunkte für einen besonderen Schutz. Es ist aber im konkreten Fall zu prüfen, ob dieser in Anspruch genommen werden kann[68].

Soweit diese behördlichen Zugriffe mit dem schweizerischen Datenschutzrecht und den schweizerischen Verfassungsgrundsätzen vereinbar sind, kann grundsätzlich davon ausgegangen werden, dass keine spezifischen darauf ausgerichteten Massnahmen nötig sind.[69] Wenn diesbezüglich Unsicherheiten bestehen, ist eine entsprechende Analyse durchzuführen[70] und es ist zu prüfen, wie eine rechtskonforme Nutzung von Cloud-Diensten mit angemessenen rechtlichen, technischen und organisatorischen Schutzmassnahmen dennoch sichergestellt werden kann (vgl. Anhang C).

In allen drei Szenarien gilt, dass das Risiko solcher Zugriffe kaum vollständig ausgeschlossen werden kann[71]:

- *Justizverfahren:* Im Rahmen von Justizverfahren wird regelmässig vorgesehen[72], dass Personen, in deren Besitz oder unter deren Kontrolle sich Daten befinden, diese nationalen Behörden unter bestimmten Voraussetzungen herauszugeben haben; weiter besteht regelmässig die Möglichkeit der Beschlagnahmung von Daten oder Hardware durch nationale Behörden. Solche Bestimmungen werden u.a. vom Übereinkommen des Europarates über Cyberkriminalität vorgegeben[73] (und sind n.b. auch in der Schweiz geltendes Recht[74]). In der Regel beste-

[64] Vgl. für WTO 20007 Pflichtenheft Ziff. 8.1.
[65] Im Rahmen der Ausschreibung WTO 20007 musste eine entsprechende Anforderung zugesichert werden; vgl. Anforderungskatalog, S. 8 (TS04)
[66] Vgl. SUVA, Antwortschreiben zur Stellungnahme EDÖB betr. M365, S. 3 f. und 7 f. m.H.
[67] Tritt ein solcher Fall ein und wurde vereinbart, dass für die Cloud-Nutzung Schweizer Recht gilt, kommt es zur Kollision. Der Cloud-Service-Provider bricht den Vertrag, was ggf. einschlägige Konsequenzen (z.B, Konventionalstrafen) auslöst.
[68] Diesbezüglich laufen Abklärungen des EDA (DV), ob mit relevanten Staaten ein gemeinsames Verständnis für die Rolle der Staatenimmunität in diesem Bereich behördlicher Daten erreicht werden kann. Ist dies der Fall, würden Behördendaten der Bundesverwaltung weiterer Stellen der öffentlichen Verwaltung in der Schweiz völkerrechtlich vor Zugriff anderer Staaten besonders geschützt.
[69] Hier sind insbesondere die Verfassungsmässigen Grundsätze, wie das Legalitätsprinzip (Art. 5 BV); das Verhältnismässigkeitsprinzip (Art. 5 Abs. 2 BV, Art. 4 Abs. 2 DSG) oder die Rechtsweggarantie und der Zugang zu einem unparteiischen Gericht (Art. 29 ff. BV und Art. 15 DSG) angesprochen.
[70] Ein strukturiertes Analyseinstrument, dass als «gute Praxis» gelten kann, hat DAVID ROSENTHAL entwickelt: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
[71] Für eine Darstellung der verschiedenen Formen vgl. auch ROSENTHAL, FAQ Nr. 28.
[72] Vgl. insbesondere auch Art. 18 Abs. 1 Cybercrime Convention und den Stored Communications Act.
[73] Vgl. Art. 18 Abs. 1 des Übereinkommens über die Cyberkriminalität vom 23. November 2001, SR 0.311.43; für die Schweiz in Kraft seit 1.1.2012; aber z.B. auch den US-Stored Communications Act.
[74] Vgl. zur Rechtslage betr. Behördenzugriffe in der Schweiz auch die Ausführungen bei LAUX/HOFFMANN, Rz. 120 ff.

hen verfahrensmässige Sicherungen zu Gunsten von Daten, namentlich, wenn es sich um Behördendaten anderer Staaten handelt.

- *Präventive Zwecke, insbesondere Terrorismusbekämpfung:* Charakteristisch für bestimmte Rechtsgrundlagen, die in den letzten Jahren insbesondere zum Zweck der Terrorismusbekämpfung geschaffen wurden, ist die verdeckte Beschaffung von Daten, die bei Kommunikationsdienstleistern gespeichert sind («at rest mass surveillance» z.B. für die USA Foreign Intelligence Surveillance Act [FISA] Section 702[75]). Diese findet in der Regel ohne Wissen der Betroffenen und ggf. auch ohne Wissen des «Datenherrn» statt. Deren Rechte können indessen zumindest teilweise durch den CSP wahrgenommen werden. In bestimmten Fällen wird dieses Risiko besonders gewichtet werden müssen (Durchführung eines RINA-Prozesses).

- *Aufklärung ausländischer Kommunikation (Funk, Kabel) und weitere nachrichtendienstliche Aktivitäten:* Zahlreiche Staaten[76] verfügen über gesetzliche Grundlagen, welche eine Aufklärung bzw. ein Abhören von Kommunikation erlauben, die im Ausland unter Zielpersonen ausländischer Nationalitäten stattfindet. Diesem Risiko unterliegt grundsätzlich jede Übermittlung von Daten zwischen Cloud-Nutzer und Cloud-Service-Provider, soweit nicht sichergestellt werden kann, dass sie nur im Inland stattfindet. *Gezielte* nachrichtendienstliche Datenzugriffe aus dem Ausland sind grundsätzlich überall möglich, sogar wenn Daten in besonders gesicherten eigenen Rechenzentren bearbeitet werden[77].

Nachstehend findet sich je eine weiterführende Kurzanalyse zur EU sowie zu den USA und China. Diese Beispiele werden gewählt, weil es sich einerseits um die Sitzstaaten von Mutter- bzw. Tochtergesellschaften der wichtigsten CSP (sog. «Hyperscaler») handelt und sich andererseits die Frage von Behördenzugriffen aufgrund von besonderen gesetzlichen Regelungen, welche vom Schweizer Recht und dem europäischen «acquis» abweichen, in diesen Jurisdiktionen besonders stellen. Zu beachten ist insbesondere, dass europäische Tochtergesellschaften von Gesellschaften mit Sitz in diesen Staaten solchen Regeln nicht unmittelbar bzw. nicht zwingend unterstehen. Diesbezüglich sind allenfalls vertragliche Vereinbarungen vorzusehen[78].

Soweit damit zu rechnen ist, dass diesbezügliche Restrisiken verbleiben könnten, sind diese nach der hier vertretenen Ansicht mit geeigneten Massnahmen auf ein akzeptables Mass zu senken.

In diesem Zusammenhang sei darauf hingewiesen, dass der Eidg. Datenschutz- und Öffentlichkeitsbbeauftragte eine abweichende Rechtsauffassung vertritt. Er lehnt seine Haltung einer jüngst etablierten strengen Praxis einiger EU-Datenschutzbehörden an, die sich auf die Rechtsprechung des EUGH, berufen[79]. Er stellt insbesondere in Frage, ob das geltende und neue Datenschutzrecht des Bundes Raum für einen risikobasierten Ansatz lassen, wenn die Rechtmässigkeit einer Auftragsdatenbearbeitung von Schweizer Behördendaten zu beurteilen ist, die Berührungen zu einem ausländischen Staat aufweist, nach dessen Recht und Behördenpraxis es zu einem intransparenten Datenzugriff kommen könnte. Nach der hier - angelehnt an die nachvollziehbar begründete Rechtsauffassung von mehreren spezialisierten Rechtsexperten[80] - vertretenen Meinung gibt es indessen überzeugende juristische und praktische Argumente, welche für eine differenziertere Position sprechen[81]. Namentlich ist den einschlägigen Bestimmungen des schweizerischen Datenschutzrechts nicht zu entnehmen, dass für Behörden bei der Auftragsdatenbearbeitung oder bei der Auslandbekanntgabe ein risikobasierter Ansatz nicht zulässig wäre[82].

---

[75] Auch die Schweiz kennt Rechtsgrundlagen, welche eine verdeckte Datensbeschaffung erlauben, vgl. heute insbesondere Art. 26 Abs. 2 und 33 Nachrichtendienstgesetz; SR 121.
[76] Auch die Schweiz hat eine gesetzliche Grundlage für die Betreibung von Funkaufklärung, vgl. Art. 38 ff. Nachrichtendienstgesetz.
[77] Vgl. dazu auch ROSENTHAL, FAQ Nr. 34. Was die gezielte nachrichtendienstliche Ausspähung betrifft, so ist eine solche selbst bei Hochsicherheits-on-premise-Lösungen nicht ausgeschlossen; vgl. z.B. NICOLE PERLROTH, The Cyber Weapons Arms Race, London 2021, S. 320 ff.
[78] Vgl. SUVA, Antwortschreiben zur Stellungnahme EDÖB betr. M365, S. 7 f. m.H.
[79] Die kritische Haltung des EDÖB zum risikobasierten Ansatz für Datenbekanntgaben ins Ausland wurde kürzlich hier dokumentiert; vgl. Auslagerung von Personendaten durch die Suva in eine Microsoft Cloud (Mitteilung vom 13.06.2022; https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1587794875) .
[80] CHRISTIAN LAUX / ALEXANDER HOFFMANN, DAVID ROSENTHAL, DAVID VASELLA.
[81] Die Gegenargumente wurde seitens SUVA (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2022/Antwort.%20Suva,%20Luzern%2020220513.%20Risikobeurteilung%20Projekt%20Digital%20Workplace%20_M365_.pdf.download.pdf/Antwort.%20Suva,%20Luzern%2020220513.%20Risikobeurteilung%20Projekt%20Digital%20Workplace%20_M365_.pdf) und der Lehre entgegnet, vgl. insbesondere DANIEL VASELLA, EDÖB, Zweifel am risikobasierten Ansatz, datenrecht.ch 13.6.2022 (https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/). Hier wird der Auffassung gefolgt, wie sie insbesondere die SUVA vertreten hat. Zur Risikoeinschätzung vgl. die bei ROSENTHAL, Mit Berufsgeheimnissen in die Cloud. beschriebene Methodik; sowie die jüngst erschienenen FAQ dazu, insbesondere Nr. 28 ff. Vgl. weiter auch CHRISTIAN LAUX / ALEXANDER HOFFMANN, Rechtmässigkeit von Public Cloud Services. Rechtsgutachten, insbesondere RZ 2015. Da es in der Schweiz zur Zeit noch keine Rechtsprechung betreffend behördliche Cloud-Sourcings gibt, verbleibt ein Risiko einer abweichenden Beurteilung durch ein Gericht.
[82] Neben den zitierten Experten geht auch das privatim-Merkblatt soweit ersichtlich nicht davon aus, dass ein risikobasierter Ansatz unzulässig wäre. Siehe ebenfalls FAQ zum Einsatz von Cloud-Technologien (www.vud.ch/view/data/2124/Div. Dokumente/220826_VUD_FAQ zum Einsatz von Cloud.pdf), welche den risikobasierten Ansatz explizit anerkennen.

1.7.1 Rechtslage EU-Mitgliedstaaten

Die Übermittlung von Personendaten aus der Schweiz an Empfänger, die in EU-Staaten domiziliert sind, ist datenschutzrechtlich grundsätzlich ohne weiteres möglich. Die europäische Datenschutzgrundverordnung entspricht einem Standard, aus dem sich auch die Regeln des nDSG ableiten. Gemäss der Länderliste des EDÖB verfügen die Mitgliedstaaten der EU über eine angemessene Datenschutzgesetzgebung.

Auch in EU-Staaten (mit Ausnahme von Irland sind alle Mitgliedstaaten dem Übereinkommen Cyberkriminalität des Europarats beigetreten[83]) bestehen dennoch Risiken, dass es im Rahmen von Justizverfahren, zu präventiven Zwecken und im Rahmen von Auslandüberwachungsmassnahmen zu Behördenzugriffen auf Daten kommen kann. Grundsätzlich kann trotzdem davon ausgegangen werden, dass in EU-Staaten keine besonderen rechtlichen Risiken bestehen und betreffend solcher Behördenzugriffe hinreichende verfahrensrechtliche Garantien bestehen. Gegebenenfalls ist zu prüfen, ob politische oder andere Risiken vorliegen (vgl. Anhang C).

1.7.2 Rechtslage USA

Für die USA stellt sich die Frage aufgrund gewisser nachrichtendienstlicher Überwachungsprogramme[84] («Geheimdienstzugriffe») sowie der im US CLOUD-Act vorgesehenen Möglichkeit für Strafverfolgungsbehörden, auf Daten beim Cloud-Anbieter zuzugreifen, ohne dass ein Rechtshilfeverfahren durchgeführt werden muss («Zugriffe durch Justizbehörden»). Der US CLOUD-Act und der Foreign Intelligence Surveillance Act (FISA) werden oft als erhebliche Risiken wahrgenommen[85]. Diese Gesetze ermöglichen in gewissen Fällen Datenzugriffe für amerikanische Behörden, auch dann, wenn diese Daten ausserhalb der USA bearbeitet bzw. gehostet werden, namentlich von Firmen mit Sitz in den USA oder mit anderen rechtlichen Beziehungen zur USA («incorporated in the United States»)[86]..

Grundsätzlich fallen auch die europäischen Töchter von amerikanischen Firmen unter diese Bestimmungen (in vielen Konstellationen indessen greifen Ausnahmen[87]). Allerdings kann eine direkt an sie adressierte Herausgabeanordnung der US-Strafverfolgungsbehörden ausserhalb des US-Territoriums nicht mit strafprozessualem Zwang durchgesetzt werden. Daher werden die US-Strafverfolgungsbehörden ihre Herausgabeanordnungen aller Voraussicht nach an die in den USA angesiedelten Mutterkonzerne richten. Ob es sodann zu einer Herausgabe der Daten von der europäischen Tochter an die amerikanische Mutter kommt, dürfte in der Praxis auch vom wirtschaftlichen Druck abhängen, den die Mutter auf die Tochter ausübt bzw. ausüben kann. Inwiefern in diesem Kontext vertragliche Abreden zwischen dem Kunden und der europäischen Tochter einen wirksamen Schutz vor der Herausgabe zu bringen vermögen, wird sich weisen; vertragliche Abreden sind daher mit anderen Schutzmechanismen zu kombinieren.

Justizverfahren: CLOUD Act

Die behördlichen Massnahmen nach dem US-CLOUD Act sind an bestimmte Voraussetzungen gebunden: So können nur Strafverfolgungsbehörden zur Verfolgung schwerer Straftaten gestützt auf den CLOUD Act vorgehen. Daten müssen von den Cloud-Service-Providern nur dann herausgegeben werden, wenn sie darüber faktische oder rechtliche Kontrolle haben[88]. All diese Begriffe entspringen allerdings dem US-Recht und werden von den US-Strafverfolgungsbehörden gemäss dem amerikanischen Verständnis angewendet. Die Cloud-Service-Provider können die Massnahmen vor einem US-Gericht anfechten; es bestehen verfahrensrechtliche Sicherungen[89]. In der Schweiz besteht kein Rechtsschutz; ob der nur im Ausland stattfindende Rechtsschutz mit dem höherrangigen Recht der Schweiz (insb. Bundesverfassung) vereinbar ist, ist zweifelhaft.[90].

---

[83] Vgl. die Übersicht hier: https://www.coe.int/en/web/cybercrime/the-budapest-convention (8.8.2022)
[84] Vgl. dazu Urteil des EugH Schrems II: CURIA - Dokumente (europa.eu) und ebenfalls FAQ zum Einsatz von Cloud-Technologien (www.vud.ch/view/data/2124/Div. Dokumente/220826_VUD_FAQ zum Einsatz von Cloud.pdf), welche den risikobasierten Ansatz explizit anerkennen.
[85] ROTH, Cloud-basierte Dienstleistungen im Licht der DSGVO, S. 68; vgl. dazu auch BRAUNECK Europa-Cloud: Zwingt der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe? Oder ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act
[86] Vgl. Bundesamt für Justiz, Bericht zum US CLOUD Act, S. 6, m.Hinw.a. ein Papier des US Department of Justice.
[87] Vgl. ROSENTHAL, FAQ Nr. 32, 35 und 36.
[88] ROSENTHAL, FAQ Nr. 35. Gemäss dem Bericht des Bundesamtes für Justiz ist entscheidend, dass der Cloud-Service-Provider nicht auf den Schlüssel zugreifen kann; vgl.Bundesamt für Justiz, a.a.O., S. 45 f.
[89] Vgl. Z.B. Neue Massnahmen zum Schutz Ihrer Daten – Microsoft Schweiz Newsroom; auch ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, S. 40 und FAQ Nr. 29. Eine ausführliche Beschreibung der Abläufe findet sich bei LAUX/HOFFMANN, S. 42 ff.
[90] Vgl. Bundesamt für Justiz, Bericht zum US CLOUD Act, S. 29 ff., 38 f.

Das Risiko eines Behördenzugriffs kann indessen erheblich gesenkt werden, wenn mit technischen Massnahmen verhindert wird, dass der Cloud-Anbieter Zugriff auf die Daten erhält. Cloud-Service-Provider können nicht zur Entschlüsselung von Daten gezwungen werden, wenn sie nicht über die Schlüssel verfügen, sondern nur der Cloud-Nutzer.

Die Herausgabe von Inhaltsdaten in solchen Verfahren ist sehr selten[91].

Präventive Zwecke und Auslandüberwachung (FISA und Executive Order 12.333)

Der Foreign Intelligence Surveillance Act (FISA) erlaubt gewissen Behörden die Beschaffung von ausländischen Informationen. Gemäss Abschnitt 702 dürfen der Attorney General und der Director of National Intelligence die Informationsbeschaffung über bestimmte Zielpersonen bewilligen, wenn davon ausgegangen werden kann, dass diese sich nicht in den USA befinden. In diesen Fällen werden Kommunikationsdienstleister verpflichtet, die bei Ihnen vorhandenen Daten zu durchsuchen[92].

Für Datenzugriffe gemäss FISA bestehen dagegen nur beschränkte verfahrensrechtlichen Sicherungen. Daten, die von ausländische Behörden stammen, geniessen unter Umständen einen gewissen Schutz, der aber nicht in jedem Fall den Anforderungen genügen kann, die sich aus dem schweizerischen Recht insbesondere bezüglich Datenschutz ergeben[93]. Zudem ist die Transparenz nicht gewährleistet, soweit die Cloud-Service-Provider keine Auskunft darüber geben dürfen, dass eine Behörde Datenzugang verlangt («gag order»). Die Cloud-Service-Provider haben rechtliche Möglichkeiten, gegen Überwachungsanordnungen vorzugehen[94].

Es bestehen indessen auch hier Voraussetzungen, welche erfüllt sein müssen (namentlich betreffend den Status des CSP als Kommunikationsdienstleister und die Tatsache, dass US-Personen von den Überwachungsmassnahmen erfasst werden dürfen) und die einer risikoorientierten Beurteilung zugänglich sind[95]. Auch hier kann zudem mit technischen Massnahmen (hinreichend starke Verschlüsselung) erreicht werden, dass nicht auf Dateninhalte im Klartext zugegriffen werden kann[96].

EO 12.333 ist ausgerichtet auf die Beschaffung von Daten während ihrer Übermittlung (*data in transit*). Die Voraussetzungen sind ähnlich definiert wie bei FISA Section 702. Soweit diese Daten bei der Übermittlung hinreichend stark verschlüsselt sind und die involvierten Kommunikationsdienstleister keinen Zugriff auf die Schlüssel haben, besteht grundsätzlich kein erhöhtes Risiko[97].

Schlussfolgerungen

Es gibt Hinweise im US-Recht, dass hinsichtlich des Datenzugriffs durch US-Behörden die Daten, die von einer ausländischen (z.B. schweizerischen) Behörde bei einem den einschlägigen US-Gesetzen unterstehenden Cloud-Service-Provider gespeichert werden, gegen Datenzugriffe gestützt auf den US CLOUD Act besonderen Schutz geniessen und zudem entsprechende Verfahrensmechanismen bestehen (z.B. nach den Prinzipien der Common-Law Comity Analysis oder dem US Foreign Sovereign Immunities Act)[98]. Die US-Gerichte entscheiden über die Anwendung dieser Regeln im Rahmen der Federal Rules of Criminal Procedure an; eine absolute Garantie für den Schutz der Schweizer Souveränität besteht daher nicht ohne Weiteres. Die Schweizer Bundesbehörde muss in diesem Rahmen sicherstellen, dass der Cloud-Service-Provider im Fall einer solchen Behördenanfrage im Verfahren meldet, dass ihr Kunde ein ausländischer Staat ist, der Souveränität beansprucht[99].

Es ist aufgrund dieser aktuellen Rechtslage im Einzelfall zu beurteilen, ob mit einer Kombination der in den einschlägigen Grundlagen und Mechanismen im US-Recht vorgesehenen Voraussetzungen, vertraglichen Vereinbarungen (insbesondere der Verpflichtung des Providers, Herausgaben gerichtlich in den USA anzufechten) und technischen Schutzmassnahmen, kann grundsätzlich auch gegen Zugriffe nach FISA und EO 12.333 ein aus rechtlicher Sicht vertretbares Risiko eines aus Schweizer Sicht

---

[91] Vgl. z.B. LAUX/HOFFMANN Rz. 208 ff. Law Enforcement Request Report | Microsoft CSR; Vgl. ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, S. 33 f.
[92] Ausführlich dazu ROSENTHAL, FAQ Nr. 29.
[93] Derzeit Gegenstand von Abklärungen im EDA. Daten im diplomatischen und konsularischen Kontext sind völkerrechtlich geschützt.
[94] ROSENTHAL, FAQ, Nr. 29, insbesondere *in fine*.
[95] Vgl. VASELLA; a.A. Merkblatt privatim, Ziff. 2.2. Detailliert mit verschiedenen Fallunterscheidungen ROSENTHAL, FAQ Nr. 29.
[96] ROSENTHAL, FAQ Nr. 32 und 35.
[97] ROSENTHAL, FAQ Nr. 29.
[98] Vgl. LAUX/HOFFMANN, Rz. 205 f., 215 sowie SUVA, S. 3 f.
[99] Dabei ist allerdings zu berücksichtigen, dass der Entscheid über allfällige Immunitäten alleinig bei US-amerikanischen Behörden liegt, bis anhin ohne jegliche Mitwirkung der Schweiz. Aktuell laufen diesbezüglich Abklärungen des EJPD und des EDA mit den zuständigen amerikanischen Behörden. Dies ist auch Teil der weitergehenden Abklärungen zur Frage, inwiefern das bestehende völkerrechtliche Institut der Staatenimmunität Behördendaten einem besonderen Schutz unterstellt (ebenso wie Daten von internationalen Organisationen und diplomatischen sowie konsularischen Vertretungen).

nicht rechtskonformen Datenzugriffs erreicht werden. Eine entsprechende Prüfung ist deshalb immer gemäss den konkreten Umständen vorzunehmen.

1.7.3 Rechtslage China

Für das Beispiel China ist schwierig einzuschätzen, wie gross die Risiken von Behördenzugriffen sind. Dass auf Daten, die in China oder von chinesischen Cloud-Service-Providern im Ausland gespeichert werden, ohne verlässliche verfahrensrechtliche Sicherungen durch chinesische Behörden zugegriffen werden kann oder dass diese blockiert werden könnten, kann nicht ausgeschlossen werden[100]. Eine diesbezügliche Beurteilung scheint auch schwierig aufgrund der grossen Vielzahl von gesetzlichen Grundlagen, welche für einen Datenzugriff in Frage kommen können[101].

Ein Routing von «data in transit» via China könnte allenfalls, auch aufgrund der besonderen Merkmale der Anbindung des chinesischen Binnennetzes an das weltweite Internet, zudem besondere Risiken bezüglich Verfügbarkeit und Integrität der Daten beinhalten[102].

Aufgrund des chinesischen Datensicherheitsgesetzes ist weiter davon auszugehen, dass den chinesischen Behörden zwingend Zugriff auf Daten zu ermöglichen ist und einmal in China gehostete Daten u.U. bei Bedarf nicht aus China zurück in die Schweiz oder in andere Staaten verschoben werden können[103], allenfalls ist sogar die Datenverschlüsselung an sich unzulässig, jedenfalls soweit Behörden dadurch keinen Zugriff mehr hätten. Zudem verbietet das chinesische Recht grundsätzlich die Verwendung von mit VPN gesicherten Verbindungen[104].

Bereits aus diesen Gründen ist eine Übermittlung von Personendaten nach China mit erheblichen und nur schwer beurteilbaren Risiken verbunden und dürfte kaum mit den Anforderungen des schweizerischen Datenschutzrechts sowie weiterer gesetzlicher Anforderungen zu vereinbaren sein.

Eine Übermittlung von Personendaten an eine Tochter einer chinesischen Muttergesellschaft wäre sorgfältig unter dem Aspekt zu prüfen, ob und unter welchen Voraussetzungen ein Zugriff der chinesischen Mutter oder durch chinesische staatliche Behörden auf Daten möglich ist, die unter der Kontrolle der Tochtergesellschaft stehen.

1.7.4 Allgemeine weitere (politische) Risiken bei Cloud-Lösungen im Ausland

Weitere (insbesondere politische) Risiken, die mit Blick auf eine Cloud-Lösung im Ausland evaluiert und soweit möglich mit entsprechenden vertraglichen Regeln soweit möglich aufgefangen werden müssen, können sein (vgl. auch Anhang C):

- Änderung der Rechtslage im betreffenden Staat, insbesondere betreffend Behördenzugriffe auf Daten: Vertragslaufzeiten angemessen definieren, ggf. "Ausstiegsklauseln" definieren.
- Standortverlagerungen in andere Staaten und daraus resultierende Änderungen des rechtlichen Rahmens: Vertragliche Garantien betreffend Hosting-Standorte vereinbaren.
- Politischer Druck auf Cloud-Service-Provider mit Blick auf Herausgabe von Daten oder Schlüsseln bzw. die Zurverfügungstellung von Nachschlüsseln (backdoors): Vorgängige Prüfung und anschliessend Beobachtung von politischen Entwicklungen.

Weiter könnte jeweils noch zu prüfen sein, ob es für bestimmte Datenbestände «souveränitätspolitische» Gründe gibt, die allenfalls dazu führen könnten, den für ein Cloud-Outsourcing bestehenden rechtlichen Spielraum nicht auszuschöpfen.

---

[100] Vgl. auch die Hinweise bei ROSENTHAL, FAQ, Nr. 28.
[101] Vgl. etwa die Aufzählung für das Beispiel China in ROSENTHAL, EU-SCC Transfer Impact Assessment; https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx (7.8.2022).
[102] Vgl. z.B. Jonathan E. HILLMANN, The Digital Silk Road, London 2021, S. 153
[103] Vgl. z.B. Steve DICKINSON, China's new cybersecurity law: no place to hide, 11. Oktober 2020; https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/ (14.1.2022)
[104] Vgl. z.B. NZZ, China baut weltweit ersten «Freihafen für Daten», 21.1.2022, S. 23.

1.8 Rechte der Betroffenen

1.8.1 Grundsatz

Die Personen, deren Daten bearbeitet werden, haben nach dem Datenschutzgesetz individuelle Rechte. Dazu gehören namentlich das Auskunftsrecht (Art. 25 nDSG) und der Anspruch auf Unterlassung einer nicht rechtmässigen Bearbeitung bzw. Löschung nicht rechtmässig bearbeiteter Daten (Art. 41 nDSG).

Das Auskunftsrecht bezieht sich auf die bearbeiteten Personendaten als solche; den Bearbeitungszweck; die Aufbewahrungsdauer der Personendaten; die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden; gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht; gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden (Art. 25 Abs. 2 nDSG). Verantwortlich für die Auskunftserteilung ist die für die Bearbeitung zuständige Verwaltungseinheit. Sie hat sicherzustellen, dass das Auskunftsrecht gewährleistet werden kann. Gleiches gilt für das Recht auf Datenherausgabe oder -übertragung nach Artikel 28 nDSG.

Gemäss Artikel 41 Absatz 2 Buchstabe a nDSG kann, wer ein schutzwürdiges Interesse hat, verlangen, dass die Verwaltungseinheit Personendaten berichtigt, löscht oder vernichtet, wenn die Daten widerrechtlich bearbeitet werden. Schutzwürdig ist das Interesse immer dann, wenn die Person betroffen ist. Bei den eigenen Personendaten ist dies grundsätzlich immer gegeben. Unter gewissen Voraussetzungen (insbesondere wenn die Richtigkeit von Daten bestritten wird und weder die Richtigkeit noch die Unrichtigkeit festgestellt werden kann) ist die Bearbeitung einzuschränken (Art. 41 Abs. 3 Bst. a nDSG).

1.8.2 Im Cloud-Kontext

Die Umsetzung dieser Ansprüche muss auch gewährleistet sein, wenn die betreffenden Daten in einer Cloud-Umgebung bearbeitet werden. In Bezug auf Cloud-Auslagerung ist deswegen namentlich sicherzustellen, dass Daten zuverlässig gelöscht (oder allenfalls vernichtet) werden können. Der Cloud-Service-Provider muss gegebenenfalls explizit vertraglich dazu verpflichtet werden, die unwiderrufliche Löschung von Daten zu gewährleisten.

2 Amtsgeheimnis

2.1 Allgemeine Bemerkungen

Das Amtsgeheimnis verfolgt hauptsächlich zwei Zwecke, und schützt zum einen den Bürger und seine Geheimnisse und zum anderen die Verwaltung, um eine ungehinderte Amtstätigkeit garantieren zu können. Es ist für Mitarbeitende der Bundesverwaltung in Artikel 320 StGB verankert und in Art. 22 Bundespersonalgesetz (BPG, SR 172.220.1) nochmals erwähnt. Für die Angestellten der Bundesverwaltung sind Geheimhaltungspflichten teilweise auch in bereichsspezifischen Bestimmungen des Bundesrechts festgehalten (bspw. Artikel 61 ff. Heilmittelgesetz). An dieser Stelle wird schwergewichtig die Verletzung des Amtsgeheimnisses gemäss Artikel 320 StGB im Vordergrund stehen, welcher die strafrechtlichen Konsequenzen festlegt.[105]

Das Öffentlichkeitsgesetz vom 17. Dezember 2004 (BGÖ; SR 152.3) spiegelt den Amtsgeheimnisbegriff und beschränkt die «Reichweite» des Amtsgeheimnisses[106]. Mit der Einführung des Öffentlichkeitsprinzips in der Bundesverwaltung hat sich der Kreis der Informationen, welche dem Amtsgeheimnis unterstehen (können) bereits stark reduziert. Eine Geheimhaltungspflicht liegt auch gemäss BGÖ dann vor, wenn:

- eine spezialgesetzliche Geheimhaltungsregelung besteht (Artikel 4) oder
- eine Ausnahme vom Öffentlichkeitsprinzip vorliegt (Artikel 3, 7 und 8 BGÖ).[107]

[105] Es sei hier noch erwähnt, dass es neben Artikel 320 StGB noch weitere Strafrechtsbestimmungen relevant sein können, so zb. Artikel 267 StGB (diplomatischer Landesverrat). Da dieser Artikel jedoch seit Jahrzehnten kaum angewandt wird, wird auf eine vertieftere Auseinandersetzung mit dieser Bestimmung zum jetzigen Zeitpunkt verzichtet.
[106] Vgl. zu dieser Abgrenzung auch BJ/EDÖB, Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen https://www.edoeb.admin.ch/edoeb/de/home/oeffentlichkeitsprinzip/dokumentation---hilfsmittel/faq-zur-umsetzung-des-oeffentlichkeitsprinzips.html), Ziff. 1.1.2 und 1.1.3 (20.6.2022).

Eine allenfalls bestehende Klassifizierung von Informationen bedeutet dabei noch nicht in jedem Fall, dass diese auch dem Amtsgeheimnis unterstehen. Das gilt insbesondere für Informationen, die INTERN klassifiziert sind (vgl. Art. 13 Abs. 3 ISchV sowie Ziff. 5 unten).

2.2 Der Tatbestand der Amtsgeheimnisverletzung (Art. 320 StGB)

2.2.1 Tatbestandselemente

Bis heute besteht eine erhebliche rechtliche Unsicherheit darüber, ob die Bearbeitung von Daten die dem Amtsgeheimnis unterstehen durch einen externen Dienstleister eine Amtsgeheimnisverletzung darstellt. Um dieser Unsicherheit Rechnung zu tragen, wird die Strafbarkeit der Amtsgeheimnisverletzung neu auch auf Hilfspersonen ausgedehnt (analog zu den Berufsgeheimnissen nach Art. 321 StGB). Dieser neue Artikel 320 StGB, der mit dem Informationssicherheitsgesetz beschlossen wurde (vgl. unten Ziff. 4.2) soll vorzeitig in Kraft gesetzt werden und auf den 1. Januar 2023 in Kraft treten. Aus diesem Grund wird die nachfolgende Analyse bereits unter neuem Recht beleuchtet.
Gemäss Artikel 320 Ziffer 1 nStGB ist strafbar, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung oder als Hilfsperson eines Beamten oder einer Behörde wahrgenommen hat.
Folgende Voraussetzungen müssen für den Tatbestand der Amtsgeheimnisverletzung kumulativ erfüllt sein:

- Täter kann ein Beamter nach Artikel 110 Absatz 3 StGB[108] sein oder eine Hilfsperson eines Beamten. Die Legaldefinition erfasst institutionelle und funktionelle Beamte.[109]
- Als Geheimnis gilt jede Tatsache, die weder offenkundig noch allgemein zugänglich ist (relative Unbekanntheit) und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat und die er tatsächlich geheim halten will (materieller Geheimnisbegriff).[110]
- Die Tathandlung besteht im Offenbaren des Amtsgeheimnisses. Offenbaren bedeutet, das Geheimnis einem Dritten zugänglichmachen, für welchen diese Information nicht bestimmt ist.[111]
- Der Vollständigkeit halber sei hier erwähnt, dass die Erfüllung des Tatbestandes stets einen Vorsatz hinsichtlich der Offenbarung des Geheimnisses voraussetzt, wobei Eventualvorsatz genügt.

2.2.2 Beurteilung der Tatbestandselemente im Cloud-Kontext

2.2.2.1 Geheimnischarakter an einem CSP übergebenen Daten

Grundsätzlich ist festzuhalten, dass die Bekanntgabe von Daten an den CSP rechtlich erlaubt ist, da er zur Geheimhaltung nach Artikel 320 Ziffer 1 nStGB verpflichtet ist. Sowohl Artikel10a DSG als auch Art. 11 VDTI sehen eine Datenbearbeitung durch Dritte unter gewissen Voraussetzungen ausdrücklich vor. Art. 10a DSG macht zwar einen Vorbehalt hinsichtlich gesetzlicher oder vertraglicher Geheimhaltungspflichten. Diese, darunter auch das Amtsgeheimnis, schliessen die Bearbeitung von Personendaten durch Dritte aber nicht grundsätzlich aus.[112] Artikel 320 nStGB steht einer Auftragsdatenbearbeitung im Sinne von Artikel 8 nDSG für Personendaten damit grundsätzlich nicht entgegen.[113] Vor der Nutzung einer Cloud-Lösung (oder eines anderen Outsourcing-Modells) ist in jedem Fall zu analysieren, ob die auszulagernden Daten gemäss den Regeln des BGÖ oder aufgrund anderer Bestimmungen[114] grundsätzlich zugänglich sind oder ob sie aufgrund spezifischer Rechtsgrundlagen besonderen Anforderungen an die Vertraulichkeit unterliegen (Schutzbedarfs- und Risikoanalyse, vgl. Ziff.

[108] Als Beamte gemäss Artikel 110 Absatz 3 StGB gelten die Beamten und Angestellten einer öffentlichen Verwaltung und der Rechtspflege sowie die Personen, die provisorisch ein Amt bekleiden oder provisorisch bei einer öffentlichen Verwaltung oder der Rechtspflege angestellt sind oder vorübergehend amtliche Funktionen ausüben.
[109] Dies bedeutet, dass es nicht von Bedeutung ist, in welcher Rechtsform eine Person für das Gemeinwesen tätig ist. Das Verhältnis kann öffentlich-rechtlich oder privatrechtlich sein. Entscheidend ist vielmehr die Funktion der Verrichtungen. Bestehen diese in der Erfüllung öffentlicher Aufgaben, so sind die Tätigkeiten amtlich und die sie verrichtenden Personen Beamte im Sinne des Strafrechts (135 IV 198, E.3.3.).
[110] BGE 127 IV 122; BSK StGB-Oberholzer, Art. 320 N 8.
[111] BSK StGB-Oberholzer, Art. 320 N 9.
[112] BÜHLER/RAMPINI, in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar DSG und BGÖ, Art. 10a DSG, N 1.
[113] GA WIDMER, S.20; RUDIN, Bearbeiten im Auftrag, S. 83 in: Praxiskommentar IDG Basel-Stadt.
[114] Vgl. künftig insb. Art. 10 Entwurf zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (BBl. 2022 805 https://fedlex.data.admin.ch/eli/fga/2022/805) betreffend Open Governement Data.

3.2 unten). Darauf gestützt ist festzulegen, welche angemessenen Schutzmassnahmen, insb. technische und organisatorische Massnahmen des Daten- und Informationsschutzes (Art. 11 VDTI), zu treffen sind.

2.2.2.2 Kenntnisnahme von den Informationen durch den CSP oder Dritte («Offenbarung»)

Der Zugriff des CSP auf geheime Daten muss im Rahmen eines Cloud-Outsourcing durch vertragliche, organisatorische und technische Massnahmen angemessen beschränkt bzw. soweit möglich ausgeschlossen werden. Wie weit der CSP (bzw. durch ihn beauftragte Mitarbeitende oder «Subcontractors») für seine Aufgabenerfüllung überhaupt den Dateninhalt zur Kenntnis nehmen können muss bzw. das in diesem Rahmen (theoretisch) kann, ist unter anderem abhängig vom gewählten Servicemodell. Das «Risiko» einer Kenntnisnahme dürfte in der Regel bei IaaS- und PaaS-Modellen tiefer einzuschätzen sein (weil Daten weitgehend mit vom Cloud-Nutzern definierten und betriebenen Softwarelösungen bearbeitet werden), bei SaaS-Modellen dagegen höher.

Ein Datenzugriff durch den CSP ist in gewissen Fällen möglich, da er das System, auf dem die Daten liegen, kontrolliert und daher die technischen Möglichkeiten für solche Zugriffe, zumindest in gewissen Bearbeitungsphasen (data in use) hätten. Bei Cloud-Infrastrukturen bestehen jedoch zahlreiche Massnahmen, um einen Zugriff zu verhindern oder zumindest erheblich zu erschweren. Ist ein Zugriff auf Daten nötig, so muss dieser auf das zwingende Ausmass beschränkt sein (z.B. für Supportaufgaben in gewissen Fällen und unter gewissen Voraussetzungen[115]). Sind solche Massnahmen in angemessenem Umfang ergriffen worden und insb. bei einer Verschlüsselung oder Pseudonymisierung von Daten, kann weitgehend verhindert werden, dass Daten offenbart werden.[116]

Ein Datenzugriff durch weitere Dritte (z.B. durch ausländische Behörden) muss ebenfalls durch angemessene, risikoadäquate Massnahmen angemessen reduziert werden[117].

2.2.2.3 Entbindung vom Amtsgeheimnis

Nach Art. 320 Ziff. 2 StGB ist der Täter nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde offenbart hat. Diese Einwilligung ist auf konkrete Einzelfälle zugeschnitten und darf nicht als Pauschaleinwilligung missbraucht werden.

2.2.2.4 Hilfspersonenstatus des CSP

Bei der vertraglichen Regelung zwischen Bundesverwaltung und dem Cloud-Service-Provider handelt es sich um ein Auftragsverhältnis im privatrechtlichen Sinn. Der CSP gilt aufgrund der oben dargelegten Rechtsgrundlagen für Outsourcing-Lösungen nicht als unberechtigter Dritter im Sinne von Art. 320 nStGB , sondern ist als Hilfsperson zu qualifizieren.

2.3 Schlussfolgerung

Gemäss den vorgehenden Ausführungen stellt die Auslagerung der Daten in die Cloud keine Verletzung des Amtsgeheimnisses nach Artikel 320 nStGB dar, sofern die Vorgaben von Artikel 11 VDTI beachtet werden. Mitarbeitende der Bundesverwaltung machen sich demnach bei der Auslagerung von Daten in die Cloud grundsätzlich nicht wegen Amtsgeheimnisverletzung strafbar.

Eine Verletzung des Amtsgeheimnisses ist insbesondere dann möglich, wenn der Cloud-Service-Provider seinerseits die Daten unberechtigterweise einem Dritten zur Verfügung stellt. Um dies zu verhindern, gibt es verschiedene Möglichkeiten. Daten können insb. verschlüsselt oder pseudonymisiert (vgl. Ziff. 2.2.1) oder tokenisiert werden. Der CSP müsste daher in der Regel technische Massnahmen umgehen und er würde in jedem Fall seine vertraglichen Verpflichtungen verletzen (und möglicherweise auch weitere strafrechtliche Bestimmungen, zu nennen wären etwas Art. 271 StGB [Verbotene Handlungen für einen fremden Staat][118] oder Art. 272-274 StGB [politischer, wirtschaftlicher oder militärischer Nachrichtendienst]).

[115] Z.B. wenn der Auftraggeber diesen Zugriff im Einzelfall genehmigt hat.
[116] SCHWARZENEGGER, THOUVENIN, STILLER, GEORGE, Anwaltsrevue 2019, S. 28.
[117] Vgl. Stellungnahme der Staatsanwaltschaft BS zum Projekt «M365» aus strafrechtlicher Sicht vom 19. April 2020.
[118] Vgl. dazu auch SUVA, S. 8.

Da es sich bei den CSP hauptsächlich um Unternehmen mit Sitz in Ausland handelt, stellt sich natürlich die Frage nach der Durchsetzung des schweizerischen Strafrechts bei einer Amtsgeheimnisverletzung eines Mitarbeiters einer ausländischen Unternehmung. Je nach Land dürfte eine Strafverfolgung demnach schwierig oder sogar unmöglich sein.

Sehr heikle Fragen dürften sich bei einem Outsourcing jedenfalls dann stellen, wenn ein Staat weitgehende (faktische und rechtliche) Zugriffsmöglichkeiten auf Daten bei Unternehmen in seinem Einflussbereich hat und die Verwaltung dies auch weiss.

3 Cyberrisikenverordnung (CyRV)

Mit der Regelung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) hat der Bundesrat eine Verordnung erlassen, die sich spezifisch mit den Cyberrisiken und der Informatiksicherheit des Bundes auseinandersetzt. Sie wird mit der Inkraftsetzung de ISV ausser Kraft gesetzt. Dies wird voraussichtlich Mitte 2023 der Fall sein.

In Bezug auf Cloud-Projekte ist vor allem das Sicherheitsverfahren für Informatikschutzobjekte (Art. 14b ff. CyRV) zu beachten.

3.1 Informatikschutzobjekt (Art. 3 Bst. h CyRV)

In Artikel 3 Buchstabe h definiert die CyRV Informatikschutzobjekte als Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der Informatik. Dabei können zusammenhängende Objekte zu einem Schutzobjekt gebündelt werden. Das heisst, dass Daten, die in eine Cloud ausgelagert werden, als ein Informatikschutzobjekt zusammengefasst und in einem Verlauf des Sicherheitsverfahren behandelt werden dürfen. So kann der Aufwand minimiert werden. Aus Artikel 3 Buchstabe h CyRV ist somit ersichtlich, dass neben den traditionellen IKT-Elementen (wie z.B. aktive Netzwerkkomponenten, Server und andere Produkte der Informatik) auch «Services» und namentlich «Datensammlungen» als Informatikschutzobjekte definiert werden. Damit sind jegliche Datensammlungen auf die Konformität mit der CyRV zu überprüfen, die in irgendeiner Form innerhalb der Bundesverwaltung generiert, gepflegt, outgesourced oder verantwortet werden. Es ist demzufolge abzuleiten, dass sämtliche Datensammlungen, die bei in- oder ausländischen Cloud-Service-Providern liegen, unter die CyRV fallen.

Gemäss Artikel 14b ff. CyRV müssen alle Informatikschutzobjekte mittels eines Sicherheitsverfahrens regelmässig überprüft werden.

3.2 Sicherheitsverfahren nach Kapitel 3a

Das Sicherheitsverfahren legt fest, welche Prozessschritte zur Gewährleistung der Informationssicherheit umgesetzt werden müssen. Gemäss Art. 14b Abs. 1 CyRV stellen die Verwaltungseinheiten sicher, dass alle Informatikschutzobjekte über eine aktuelle Schutzbedarfsanalyse (Schuban) vor der Projektfreigabe verfügen. Die Schuban hilft festzustellen, welche Daten mit dem Informatikschutzobjekt bearbeitet werden. Auf dieser Basis ist dann zu prüfen, welche Anforderungen erfüllt werden müssen. Artikel 14c CyRV legt weiter fest, dass die Vorgaben für den Grundschutz für Informatikschutzobjekte umgesetzt und dokumentiert werden. Artikel 14d CyRV regelt das weitere Vorgehen im Fall, dass die Schuban für die Informatikschutzobjekte einen erhöhten Schutzbedarf ausweist.

In Bezug auf Cloud-Projekte bedeutet dies, dass die potenziellen Risiken eruiert werden müssen, bevor Daten in die Cloud ausgelagert werden können (vgl. dazu Anhang C). Sollte sich aus der Schuban ein erhöhter Schutzbedarf ergeben (beispielsweise aufgrund besonders schützenwerter Daten) müssen die Verwaltungseinheiten weitere Sicherheitsmassnahmen festlegen und allfällige Restrisiken ausweisen (Art. 14d Abs. 1 und 2 CyRV) oder auf die Auslagerung verzichten.

Für Cloud-Projekte ist insbesondere im Rahmen der Schuban zu beurteilen, ob Schutzobjekte durch nachrichtendienstliche Ausspähung erheblich gefährdet werden könnten. In diesem Fall ist gleichzeitig auch ein RINA-Prozess zu durchlaufen.[119] Soweit die Cloud-Service-Provider in Staaten domiziliert sind oder zu solchen Staaten eine Verbindung haben, bei denen eine nachrichtendienstliche Ausspähung nicht ausgeschlossen werden kann, muss diese Frage vertieft geprüft werden[120]. Eine erhebliche

[119] Siehe dazu: P041-Schutzbedarfsanalyse_V4-5-d (1).pdf, S. 8 f. Der RINA-Prozess wird mit der Umsetzung ISG im Rahmen des Betriebssicherheitsverfahren abgedeckt.
[120] Das gilt insbesondere für Cloud-Outsourcings unter WTO 20007.

Gefährdung und damit die Pflicht zum Durchlauf eines RINA Prozesses ergibt sich unseres Erachtens jedoch nur dann, wenn die Daten als sensitiv (z.B. Berufs-, Geschäfts oder Fabrikationsgeheimnisse Dritter; andere heikle Personenbezogene Informationen; Daten, welche die innere und/oder äussere Sicherheit der Schweiz betreffen) eingestuft werden müssen. Bei Daten, welche allgemein öffentlich zugänglich sind, trifft diese Voraussetzung dagegen eindeutig nicht zu.

4 Bestimmungen zum Informationsschutz des Bundes

Die Informationsschutzverordnung (ISchV, SR 510.411) vom 4. Juli 2007 wird mit Inkraftsetzung des Informationssicherheitsgesetzes (ISG) in der nachgelagerte Informationssicherheitsverordnung ISV abgebildet und durch sie ersetzt werden. Der Fokus des nachfolgenden Kapitels soll auf dem geltenden Recht, der ISchV, liegen (vgl. unten Punkt 5.1). Um jedoch der Planung von langjährigen Projekten gerecht zu werden, sollen die wichtigsten Neuerungen des ISG sowie die Änderungen anderer Erlasse, welche im Zuge des ISG angepasst werden und für Cloud-Projekte relevant sein könnten, in Kapitel 5.2 in groben Zügen aufgeführt werden.

4.1 Die Informationsschutzverordnung (ISchV)

4.1.1 Inhalt

Die ISchV regelt den Schutz von Informationen des Bundes (d.h. für die Bundesverwaltung nach Art. 7 und 7a RVOG), der Armee und des Zivilschutzes (vgl. Art. 1 Abs. 1 i.V.m. Art. 4-7 ISchV). Dafür regelt die ISchV u.a. die Klassifizierung von Informationen sowie deren Bearbeitung (vgl. Bearbeitungsvorschriften nach Art. 18 i.V.m. Anhang ISchV). Die Regelungen für den grenzüberschreitenden Informationsschutz finden sich in den entsprechenden internationalen Informationsschutzabkommen[121] zwischen der Schweiz und ausländischen Partnerländern.

Wer als Angestellter der Bundesverwaltung, als Angehöriger der Armee oder des Zivilschutzes, als Organisation und Person des öffentlichen oder privaten Rechts, oder als eidgenössisches oder kantonales Gericht klassifizierte Informationen des Bundes bearbeitet, ist für die Einhaltung der Informationsschutzvorschriften verantwortlich (vgl. Art. 12 Abs. 1 ISchV); die Vorschriften zum Schutz von Personendaten nach DSG gelten unabhängig von der Anwendbarkeit der ISchV und sind separat zu prüfen bzw. sind parallel zur ISchV anwendbar.

Werden klassifizierte Informationen nach ISchV in einer Cloud bearbeitet oder neu erstellt, ist das Projekt entsprechend zu planen. Derzeit gibt es keine materiell-rechtlichen Bestimmungen, welche den Cloud-Einsatz in der Bundesverwaltung für INTERN oder VERTRAULICH per se verbieten (für GEHEIME Informationen ist die Cloud-Verwendung jedoch untersagt[122]). Mit der ISchV gelten parallel nachfolgende Bestimmungen[123]:

- Weisungen über die detaillierten Bearbeitungsvorschriften zum Informationsschutz vom 18.01.2008 (Bearbeitungsweisungen; vgl. Art. 18 Abs. 2 ISchV);
- Weisungen über die Klassifizierung vom 26.09.2011 (Klassifizierungskatalog).

4.1.2 Bearbeitung schutzwürdiger Informationen und Anwendbarkeit ISchV

Die Projektleitung muss vor Beginn des Projekts und falls notwendig auch im Verlaufe des Projekts prüfen, ob schutzwürdige Informationen betroffen und damit die ISchV anwendbar ist (Schuban gemäss Art. 14b CyRV). Die gängigen Projektmanagement-Methoden (wie HERMES) sehen dies auch ausdrücklich vor.

Bei einem Cloud-Projekt helfen folgende Überlegungen (vgl. auch Anhang E):

Wer schutzwürdige Informationen verfasst oder herausgibt, weist sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu: INTERN, VERTRAULICH, GEHEIM

[121] Internationales und Besuchswesen (admin.ch).
[122] Vgl. Zusammenstellung Vorgaben Informationsschutzmassnahmen für Mitarbeitende der Bundesverwaltung als Weisung des ISB gestützt auf ISchV vom 1.04.2020 (oranges Faltblatt).
[123] https://www.vtg.admin.ch/content/vtg-internet/de/service/info_trp/sicherheit/_jcr_content/contentPar/tabs_copy/items/downloads/tabPar/downloadlist/downloadItems/602_1472209897681.download/Reglement%2052.059%20Integrale%20Sicherheit.pdf

(vgl. Art. 4 Abs. 1 ISchV). Insofern hat die Projektleitung selber oder mit Hilfe der Informationsschutzbeauftragten oder des Informationsschutzbeauftragten seines Amtes oder Departements/BK zu prüfen, ob im Rahmen des Projekts ggf. klassifizierte Informationen bearbeitet werden oder künftig selber erstellt werden:

- Das ist einfach zu prüfen, denn der Klassifizierungsvermerk steht jeweils oben rechts zumindest immer auf der ersten Seite eines Dokuments (WordDok, Excel, PowerPoint). Einer besonderen Beurteilung unterliegen Sammelwerke, welche ggf. zu klassifizieren sind oder einer höheren Klassifizierungsstufe zugeordnet werden müssen (vgl. Art. 4 Abs. 2 ISchV). Sollte die Projektleitung vermuten, dass die zu bearbeitenden Informationen zu hoch klassifiziert sind (was in der Bundesverwaltung regelmässig beobachtet wird), besteht die Möglichkeit, die Klassifizierung einer neuen Beurteilung zu unterziehen. Diese Änderung der Klassifizierung eines Dokumentes bzw. einer Dokumentenreihe oder einer Dokumentenart darf jedoch nur durch die Person oder Amtsstelle erfolgen, in deren Interesse die Geheimhaltung liegt (sog. Geheimnisherr) und kann nicht durch die Projektleitung selbst vorgenommen werden (vgl. Art. 4 Abs. 1 ISchV). Die Änderung der Klassifizierung kann aufgrund der unterschiedlichen Bearbeitungsvorschriften nach Art. 18 ISchV für INTERN, VERTRAULICHE oder GEHEIME Informationen einen erheblichen Einfluss haben auf die technischen Schutzvorkehrungen von Systemen, Software oder Hardware, auf die notwendigen Ressourcen sowie auf die Projektkosten und damit auf den Erfolg eines Projekts, da für den Schutz von VERTRAULICH klassifizierten Informationen stärkere Schutzmassnahmen (insbesondere hinreichend starke Verschlüsselung) erforderlich sind. Dies bedeutet höhere Kosten und ggf. mehr Ressourcen für ein Projekt.
- Das erfordert seitens der Projektleitung, dass im Rahmen des Projekts künftig zu erstellende Informationen (vgl. Art. 3 Bst. a ISchV) oder Informationsträger (vgl. Art. 3 Bst. b ISchV) gemäss den geltenden Bestimmungen nach Art. 4 - 9 ISchV klassifiziert werden und die Projektmitarbeitenden entsprechend darauf aufmerksam zu machen sind. Zu berücksichtigen ist, dass durch die Zusammenfügung von Informationen oder Informationsträgern in der Cloud unvorhergesehen ein Sammelwerk entstehen kann, welches ggf. eine Anpassung der Klassifizierung bedingt oder neu ein Klassifizierungstatbestand geschaffen wird (vgl. Art. 4 Abs. 2 ISchV).

Werden schutzwürdige Informationen (INTERN, VERTRAULICH,) nach ISchV in einer Public-Cloud bearbeitet oder soll im Rahmen eines Projekts eine Cloud-Anwendung eingeführt werden, müssen nachfolgende Punkte beachtet bzw. seitens Projektleitung geprüft werden:

- **Grundfrage:** Welche Art klassifizierter Informationen soll bearbeitet werden oder werden im Rahmen des Projekts erstellt? Entsprechend kommt die ISchV samt Bearbeitungsvorschriften und Klassifizierungskatalog zur Anwendung oder eben nicht.
- **Folgefrage:** Welche anderen Bestimmungen und Weisungen des Bundes, des Departements oder der Verwaltungseinheit gelten zusätzlich zum IT-Grundschutz[124] sowie dem allgemein geltenden Recht (beispielsweise Weisungen oder Richtlinien des Bundes oder der Departemente, wie Cloud-Strategie Bund, Cloud-Strategie Departement) für die klassifizieren Informationen?

Ist die ISchV anwendbar, hat die Projektleitung namentlich sicherzustellen, dass der Sicherheitsprozess nach CyRV Art. 14d ff. i.V.m. Art. 3 Bst. h (Informatikschutzobjekt; Cloud-Service als Informatikschutzobjekt) in das Projekt integriert und korrekt durchgeführt wird. Die Rechtskonformität ist immer dann erstellt, wenn von zuständiger Stelle die ausgewiesenen Restrisiken übernommen werden. Ist das Projekt nachweislich auf dem aktuellen Stand der Wissenschaft und Technik, darf eine Risiken-Nutzen-Abwägung vorgenommen werden. Wenn diese nachvollziehbar zugunsten des Nutzens ausfällt, so ist die Übernahme der Restrisiken zulässig.

Werden im Rahmen des Cloud-Projekts keine klassifizierten Informationen bearbeitet oder erstellt (vgl. oben), so kommt die ISchV nicht zur Anwendung. Dies dürfte häufig der Fall sein, denn gemäss internen Schätzungen sind ca. 90% der Informationen der Bundesverwaltung nicht klassifiziert. Umgekehrt ist eine Anwendbarkeit auch dann gegeben, wenn nur ein kleiner Teil von Informationen, die von einem konkreten Vorhaben betroffen sind, klassifiziert sind.

[124] Per 1. März 2022 tritt der neue IT-Grundschutz in Kraft (ehemals IKT-Grundschutz).

4.2 Das künftige Informationssicherheitsgesetz (ISG)

4.2.1 Grundsätzliche Neuerungen des ISG

Das ISG soll die sichere Bearbeitung aller Informationen, für die der Bund zuständig ist (auch die nicht-klassifizierten Informationen) hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit gewährleisten und ebenfalls neu den sicheren Einsatz von Informatikmittel des Bundes gewährleisten. Gemäss der Legaldefinition nach Artikel 5 Bst. a ISG werden als Informatikmittel «Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen» bezeichnet, worunter auch Cloud-Anwendungen fallen.

Um die Informationssicherheit beim Einsatz von Informatikmitteln zu gewährleisten, insbesondere beim Bezug von Informatikdienstleistungen bei externen Leistungserbringern, sind neu die Bestimmungen zur «Sicherheit beim Einsatz von Informatikmitteln» nach Artikel 16-19 ISG massgebend (ISG 16-19 ersetzen die Artikel 14b -14e CyRV).

Das ISG hat im Vergleich zur ISchV einen erweiterten institutionellen Geltungsbereich: Das ISG gilt für alle Bundesbehörden (Parlament, Bundesrat, eidgenössische Gerichte, Bundesanwaltschaft und ihre Aufsichtsbehörde und Nationalbank; sog. Verpflichtete Behörden nach Art. 2 Abs. 1 ISG) und ihre unterstellten Organisationen (Departemente, Bundeskanzlei, zentrale und dezentrale Verwaltungseinheiten, samt Armee und Zivilschutz; sog. verpflichtete Organisationen nach Art. 2 Abs. 2 ISG). Externe öffentlich-rechtliche oder private Organisationen, die mit Bundesaufgaben betraut werden, gelten ebenfalls als verpflichtete Organisationen und sind dem ISG unterstellt. Der Bundesrat kann jedoch auf dem Verordnungsweg Organisationen der dezentralen Bundesverwaltung sowie verwaltungsexterne Organisationen des öffentlichen oder privaten Rechts, die mit Verwaltungsaufgaben betraut sind, vom Geltungsbereich des ISG oder von Teilen des ISG ausnehmen (Art. 2 Abs. 3 und 4 ISG). Ebenfalls müssen die Kantone gewisse Bestimmungen des ISG befolgen, sofern sie im Rahmen der Bearbeitung klassifizierter Informationen des Bundes oder im Rahmen eines Zugriffs auf Informatikmittel des Bundes keinen gleichwertigen Schutz gewährleisten. Dritte, welche nicht unter den Geltungsbereich des ISG fallen, sind mit vertraglichen Vereinbarungen zur Einhaltung der Bestimmungen nach ISG zu verpflichten (vgl. Artikel ISG 9) bzw. bei gegebenen Voraussetzungen dem Betriebssicherheitsverfahren zu unterziehen (Art. 49 ff. ISG).

Die Schwelle der Klassifizierungsstufen (INTERN, VERTRAULICH, GEHEIM) wird angehoben: Das heutige VERTRAULICH wird in der Tendenz das morgige INTERN. Damit wird die Anzahl klassifizierter Informationen massiv gesenkt und u.a. die Anzahl der Personensicherheitsprüfungen (PSP) reduziert. Die Klassifizierungskriterien sollen künftig in der Informationssicherheitsverordnung im Detail festgelegt werden (vgl. VE-ISV Art. 17 ff.).

Es wird neu die «sicherheitsempfindliche Tätigkeit» eingeführt (Art. 5 Bst. b ISG), die für die Durchführung von Personensicherheitsprüfungen (PSP) und von Betriebssicherheitsverfahren (BSV; ehemals Geheimschutzverfahren) massgebend ist. Sie umfasst die Bearbeitung von VERTRAULICH und GEHEIM klassifizierten Informationen (Art. 13 Abs. 2 und 3 ISG), die Verwaltung, den Betrieb, die Wartung und die Überprüfung von Informatikmitteln mit hohem und sehr hohem Schutz (Art. 17 ISG) sowie den Zugang zu Sicherheitszonen 2 und 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen.

Die Informationssicherheit soll sich künftig an internationalen Standards ausrichten, wobei ein Informationssicherheitsmanagementsystem (ISMS) samt Ambitionsniveau der Sicherheit sowie entsprechende Massnahmen definiert werden. Mit dem ISMS wird der minimal erforderliche Schutz der Information und Informatikmittel im Vergleich zu den heutigen Anforderungen nach CyRV und ISchV angehoben.

4.2.2 Laufende Arbeiten zur Umsetzung des ISG

Das ISG wurde am 20. Dezember 2020 vom Parlament verabschiedet. Am 12. April 2021 ist die Referendumsfrist unbenutzt abgelaufen. Seither werden die Ausführungsbestimmungen zum ISG unter der Federführung des GS-VBS erarbeitet mit dem Ziel, das ISG samt Verordnungen auf den 1. Juli 2023 in Kraft zu setzen[125]. Das ISG wird die ISchV und die CyRV mit dessen Inkraftsetzung ersetzen.

[125] Für sämtliche Fragen zum Stand des Projekts «Umsetzung ISG» wenden Sie sich bitte an Christophe Perron (Projektleiter) oder Melanie Koller (Stv. Projektleiterin). Gegenwärtig wird zudem eine Intranet-Seite zum ISG erarbeitet.

Zum ISG werden verschiedene Ausführungsbestimmungen erarbeitet.[126] Die ISchV soll mit Inkraftsetzung des ISG vollständig aufgehoben werden. Die CyRV (SR 120.73) soll aufgehoben und ihre Bestimmungen (teilweise angepasst) in die künftige Informationssicherheitsverordnung (ISV) integriert werden. Weiter soll die Identity und Access Management-Verordnung (IAMV, SR 172.010.59) teilrevidiert werden.

Die heutige Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) soll komplett aufgehoben und ein Teil der Bestimmungen des Bundesgesetzes über die Massnahmen der inneren Sicherheit (BWIS, SR 120) sollen in die künftige Personensicherheitsprüfungsverordnung (VPSP) integriert werden.

Die heutige Geheimschutzverordnung (SR 510.413) soll vollständig ersetzt werden durch die künftige Verordnung über das Betriebssicherheitsverfahren (VBSV). Der Anwendungsbereich des Betriebssicherheitsverfahrens (BSV) soll vom heute nur militärischen Bereich neu auch auf den zivilen Bereich erweitert werden. Damit sollen sich neu auch Private-Cloud-Service-Provider einem BSV unterziehen müssen, sofern diese für den Bund eine sicherheitsempfindliche Tätigkeit nach Art. 5 Bst. b ISG ausführen. Unter eine solche Tätigkeit fallen im vorliegenden Zusammenhang: Die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen und die Verwaltung, der Betrieb, die Wartung und die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz». Die VBSV soll auch den heutigen RINA-Prozess ersetzen. Schliesslich soll mit einer Revision des ISG eine Meldepflicht für Cyber-Vorfälle bei kritischen Infrastrukturen eingeführt werden[127].

4.2.3 Auswirkungen für Cloud-Projekte ab Inkraftsetzung des ISG

Das ISG regelt zwei Punkte, die für den Einsatz einer Cloud-Lösung in seinem Geltungsbereich massgeblich sind: Erstens betreffend die darin zu bearbeitenden Informationen (klassifizierte vs. nicht-klassifizierte Information) und zweitens betreffend das Resultat des Sicherheitsverfahrens bzw. ob ein Informatikmitten der Sicherheitsstufe «Grundschutz», «hoher Schutz» oder «sehr hoher Schutz» gemäss Artikel 17 ISG zuzuordnen ist.

Insbesondere werden folgende Punkte zu prüfen sein:

- *Klassifizierung*: Nach ISchV klassifizierte Informationen müssen mit der Inkraftsetzung des ISG an die neuen Klassifizierungsvorschriften angepasst werden (vgl. Art. 11-15 ISG i.V.m. der künftigen Informationssicherheitsverordnung (ISV)), sobald diese Informationen das erste Mal bearbeitet (beispielsweise gespeichert, angepasst, gelöscht etc.) werden (vgl. Art. 90 Abs. 1 ISG);
- Die *Informatikmittel* (vgl. Art. 5 Bst. a ISG) müssen innerhalb von zwei Jahren nach Inkraftsetzung des ISG nach den neuen Bestimmungen des ISG eingestuft werden (vgl. Art. 16-19 ISG i.V.m. der künftigen Informationssicherheitsverordnung). Technische Massnahmen zur Gewährleistung der Informationssicherheit müssen hingegen erst innerhalb von sechs Jahren nach Inkraftsetzung des ISG umgesetzt werden (vgl. Art. 90 Abs. 2 ISG). Als Informatikmittel gilt auch eine Cloud-Anwendung, womit das ISG und alle entsprechenden Ausführungsbestimmungen auf für Cloud-Projekte zur Anwendung gelangen;
- *Personensicherheitsprüfungen (PSP)*: Nach bisherigem Recht ausgestellte Sicherheits- und Risikoerklärungen sind fünf Jahre ab deren Ausstellung gültig (Art. 90 Abs. 3 ISG); d h. die Projektleitung hat hinsichtlich bestehender Prüfungen nichts zu unternehmen. Anders aber hins. neuer Mitarbeitenden im Projekt: Hier hat die Projektleitung i.Z.m. dem Auftraggeber das Recht, dass die PSP für die neuen Mitarbeitenden nach den neuen Bestimmungen des ISG erfolgen;
- *Betriebssicherheitsverfahren (BSV)*: Nach bisherigem Recht ausgestellte Betriebssicherheitserklärungen (BSE) sind fünf Jahre ab deren Ausstellung gültig (Art. 90 Abs. 3 ISG); d.h. die Projektleitung muss bei sicherheitsempfindlichen Aufträgen sicherstellen, dass der Anbieter über eine gültige BSE verfügt, ggf. unter Hinzuziehung der Fachstelle Betriebssicherheitsverfahren (vgl. Verfahren nach der VBSV). Wenn noch gar keine BSE ausgestellt wurde, ist eine entsprechende zu besorgen bzw. dies zu prüfen (vgl. Verfahren nach der BSVV). Neu sind auch Auftraggeber und Auftraggeberinnen der zivilen Bundesverwaltung gehalten, das BSV anzustossen (und nicht mehr nur das VBS gemäss der ehemaligen Geheimschutzverordnung).

[126] Zeitplan ISG-Umsetzung per Stand Mitte Januar 2022: Start Erste ÄK ca. Ende Februar 2022; Vernehmlassung 24.08. – 24.11.2022 Start IKS per Mitte 2023.
[127] Für sämtliche Fragen zum Stand der Meldepflichten für kritische Infrastrukturen wenden Sie sich bitte an: Manuel Suter (GS-EFD).

5 Weitere relevante Rechtsgrundlagen

5.1 Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

Die Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV; SR 172.010.59) regelt für IAM-Systeme, die Verzeichnisdienste und den zentralen Identitätsspeicher des Bundes die Zuständigkeiten, die Bearbeitung und Bekanntgabe von Personendaten und die Anforderungen an die Informationssicherheit (Art. 1 IAMV). Die IAMV regelt im 5. Abschnitt (Art. 15 ff. IAMV) die Datenbekanntgabe. Artikel 17 IAMV regelt sodann auch die Bekanntgabe von Personendaten an einen externen Betreiber. Gemäss Artikel 17 Absatz 1 IAMV dürfen Personendaten aus IAM-Systemen dem externen Betreiber grundsätzlich bekannt gegeben werden. Artikel 17 Absatz 2-4 IAMV nennt die Voraussetzungen und Pflichten die eingehalten werden müssen, damit die Bekanntgabe der Personendaten an externe Betreiber rechtmässig ist[128]. Artikel 18 IAMV regelt noch die Anforderungen an die Informationssicherheit. Die IAMV regelt somit bereits explizit den Fall des Cloud Outsourcings und erlaubt diesen für IAM-Systeme unter Einhaltung der in Artikel 17ff. IAMV genannten Voraussetzungen.

Die IAMV wird gegenwärtig teilrevidiert und die Änderung soll zusammen mit dem ISG auf den 1. Juli 2023 in Kraft treten. In Bezug auf die oben erwähnten Artikel sind jedoch keine Anpassungen vorgesehen (Stand: Februar 2022).

5.2 Vorschriften zur Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen

Die Artikel 57i ff. Regierungs- und Verwaltungsorganisationsgesetz (RVOG)[129] regeln die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen (sog. Randdaten) subsidiär, soweit kein anderes Bundesgesetz eine Regelung trifft. Art. 57j Abs. 1 RVOG legt den Grundsatz fest, dass Verwaltungseinheiten Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, grundsätzlich nicht aufzeichnen oder auswerten dürfen.

Die Artikel 57l – 57o RVOG regeln, wann Personendaten aufgezeichnet werden dürfen, insbesondere: Datensicherung, Wartung, Kontrolle der Einhaltung von Nutzungsreglement, Nachvollzug des Zugriffs. Artikel 57m und 57n RVOG regeln die nicht personenbezogene und nicht namentlich personenbezogene Auswertung. Art. 57o RVOG regelt die namentliche personenbezogene Auswertung. Diese ist insbesondere zulässig zur Analyse und Behebung von Störungen der elektronischen Infrastruktur und zur Abwehr konkreter Bedrohungen dieser Infrastruktur (Abs. 1 Bst. b). Auswertungen zur Abklärung von Missbräuchen sind nur durch Verwaltungseinheiten und nur nach schriftlicher Information der betroffenen Person zulässig; das Verfahren wird in der Ausführungsverordnung eingehend geregelt.

Verwaltungseinheiten sind schliesslich verpflichtet, die erforderlichen präventiven technischen und organisatorischen Massnahmen zur Verhinderung von Missbräuchen zu treffen (Art. 57p RVOG). Für Cloud-Projekte bedeutet dies namentlich, dass darauf zu achten ist, dass Randdaten (z.B. Zugriffslogs) angemessen geschützt und der Zugriff darauf klar geregelt und regelmässig überprüft werden.

Gemäss Artikel 1 der Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen («Randdatenverordnung»)[130] ist zwischen bewirtschafteten und nicht bewirtschafteten Daten zu unterscheiden. Bewirtschaftete Daten sind Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes aufgezeichnet und regelmässig genutzt, ausgewertet oder bewusst gelöscht werden. Dies gilt etwa für Zugriffslogs von Informationssystemen oder Daten über die Benutzung von Schliesssystemen. Nicht bewirtschaftete Daten sind Personendaten die bei der Nutzung der elektronischen Infrastruktur des Bundes aufgezeichnet, aber nicht oder nicht regelmässig genutzt, ausgewertet oder systematisch gelöscht werden. Nicht bewirtschaftete Daten sind beispielsweise die von einem Drucker gespeicherten Angaben über die bearbeiteten Druckaufträge.

[128] Dazu gehört unter anderem die vorgängige Information der Betroffenen Personen (Art. 17 Abs. 4 IAMV).
[129] SR 172.010
[130] SR 172.010.442

Auf bewirtschaftete Daten dürfen nur die Betreiberin oder die nach dem Datenschutzkonzept einer Verwaltungseinheit vorgesehene Stelle zugreifen. Gemäss Begriffsdefinition nach Artikel 1 Buchstabe c dieser Verordnung ist die Betreiberin, die mit dem technischen Betrieb der elektronischen Infrastruktur des Bundes beauftragte Stelle. Da Cloud-Service-Provider vom Bund beauftragt werden, gelten sie grundsätzlich als Beauftragte im Sinne der Verordnung. Sie dürfen demnach im Rahmen der gesetzlich erlaubten Zwecke auf die Randdaten zugreifen. Bei nicht bewirtschafteten Daten darf nur das Verwaltungseinheit, welches die Geräte, auf denen diese Daten aufgezeichnet werden, selbst nutzt, zugreifen.

5.3 Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung)

Die GEVER-Verordnung hat einen sehr breiten Anwendungsbereich: Sie gilt nicht nur für die zentrale Bundesverwaltung, sondern in gewissen Fällen auch für dezentrale Einheiten und sie gilt sowohl für standardisierte Geschäftsverwaltungssysteme als auch für nicht standardisierte Systeme (Art. 3).

Im Bereich der standardisierten Systeme müsste eine Cloud-Nutzung in den Standardvorgaben vorgesehen und geregelt werden. Im Bereich der nicht standardisierten Systeme sind gewisse Vorgaben der GEVER-Verordnung bei Cloud-Outsourcings zu beachten. Das gilt insbesondere für die Vorgaben zur Bearbeitung (Art. 11) und die Protokollierung (Art. 13).

5.4 Weisungen mit Geltung für die gesamte Bundesverwaltung

Verschiedene Weisungen und Richtlinien, die für die gesamte Bundesverwaltung Gültigkeit haben, können in Bezug auf das Cloud-Sourcing von Relevanz sein. Beispielhaft können hier die Einsatzrichtlinien des Bereichs DTI der BK aufgeführt werden, die sich auf Artikel 17 Absatz 1 VDTI stützen. Davon sind insbesondere die E027 – Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)[131] oder die E026 – Einsatzrichtlinie Arbeitsplatzsystem von möglicher Bedeutung[132]. Diese Einsatzrichtlinien konkretisieren jedoch übergeordnetes Recht und es ergeben sich keine neuen Rechte und Pflichten für die Verwaltungseinheiten.

Als weitere wichtige Vorgabe ist noch der IT-Grundschutz der Bundesverwaltung[133] zu nennen, der für alle Verwaltungseinheiten verbindlich einzuhalten ist und sich auf Artikel 11, Absatz 1, Buchstabe e CyRV stützt (vgl. Teil 2, Ziff. 0).

[131] Einsatzrichtlinie E027 1-1 (1).pdf.
[132] E026 1-1 GENEHMIGT d (1).pdf.
[133] Si001-IT-Grundschutz_V5-0-d (4).pdf.

Anhang A Literatur und Materialien

BAERISWYL BRUNO	Wenn die Rechtsauslegung «nebulös» wird, in: digma 2019
BISCHOF SARAH	Teil 2: Die Bekanntgabe von Gesundheitsdaten / Kapitel 3: Datenschutzkonforme Bearbeitung von Gesundheitsdaten / V. Die datenschutzrechtlichen Grundsätze bei der Datenbekanntgabe / 1. - 6.; in: Datenschutz und Berufsgeheimnis im ambulanten Leistungsbereich (2020)
BLÖCHLINGER KARIN	Amtsgeheimnis und Öffentlichkeitsprinzip im Spannungsverhältnis, in: iusNet 2021
BRAUNECK JENS	Europa-Cloud: Zwingt der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe? In: Europäisches Wirtschafts- und Steuerrecht, 2019
Bundesamt für Justiz	Bericht zum US CLOUD Act, 2021
DICKINSON STEVE	China's new cybersecurity law: no place to hide, 11. Oktober 2020; https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/ (24.3.2022)
HILLMANN JONATHAN E.	Digital Silk Road (2021)
KONFERENZ DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN PRIVATIM	Merkblatt Cloud-spezifische Risiken und Massnahmen (V3 / 03.02.2022 (zit. Merkblatt privatim)
LAUX CHRISTIAN / HOFFMANN ALEXANDER	Rechtmässigkeit von Public Cloud Services, «Cloud-Gutachten» (unter Berücksichtigung des CLOUD Act), Rechtsgutachten an Organisation und Informatik der Stadt Zürich, 16. September 2021 (Link: Cloud Gutachten LLAG für OIZ (Sep 2021) mit Zusätzen (Nov 2021) (lauxlawyers.ch))
MICHLIG MATTHIAS; WYLER EVA	Art. 320 Verletzung des Amtsgeheimnisses, in: StGB annotierter Kommentar (2020)
MILLARD CHRISTOPHER	Cloud Computing Law, 2nd ed., Oxford University Press (2021)
ROSENTHAL DAVID	Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act; in: Jusletter 10. August 2020
ROSENTHAL DAVID	Schweizer Banken in die Cloud; Vischer 9. September 2021 https://www.vischer.com/know-how/blog/schweizer-banken-in-die-cloud-so-geht-es-und-so-nicht-39214/
ROSENTHAL DAVID	Frequently Asked Questions (FAQ) on the Risk of Foreign Lawful Access and the Statistical “Rosenthal” Method for Assessing it, Version 1. August 2022, https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf (9.8.2022)
ROTH DAVID	Cloud-basierte Dienstleistungen im Licht der DSGVO in: Aktuelle Juristische Praxis, 2020
RUDIN BEAT	Bearbeiten im Auftrag in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), (2014)
SCHWARZENEGGER CHRISTIAN; THOUVENIN FLORENT; STILLER BURKHARD; GEORGE DAMIAN	Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, in: Anwaltsrevue 1/2019

STEINER THOMAS	Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, in: sic! 2020
THALNER CAROLINE	Das moderne Amtsgeheimnis im Spannungsfeld des Öffentlichkeitsprinzips, Masterarbeit UZH, 2019
VASELLA DAVID	Privatim – Merkblatt «Cloud-spezifische Risiken und Massnahmen» für öffentliche Organe: neue Fassung und kritische Anmerkungen; https://datenrecht.ch/privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-neue-fassung-und-kritische-anmerkungen/ (22.3.2022)
WIDMER URSULA	Gutachten Klärung und Analyse der rechtlichen Grundlagen für die Integration von «Platform-as-a-Service» und «Software-as-a-Service» in der öffentlichen Verwaltung für die Schweizerische Informatikkonferenz (SIK), 2018
WOHLERS WOLFGANG	Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), in: digma – Schriften zum Datenrecht Band/Nr. 9

Anhang B Glossar

Schlüsselmanagement:	Die Verschlüsselungsstärke sollte den spezifischen Zeitraum berücksichtigen, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist. Der Verschlüsselungsalgorithmus sollte fehlerfrei durch ordnungsgemäss gepflegte Software implementiert sein, deren Konformität mit der Spezifikation des ausgewählten Algorithmus (z. B. durch Zertifizierung) bestätigt wurde. Die Schlüssel sollten zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden. **Bring Your Own Key (BYOK) oder Bring Your Own Encription (BYOE):** Die Verwaltungseinheit bringt die Verschlüsselungsschlüssel selbst mit und übergibt diese aber dem Cloud-Service-Provider zur Verwaltung und Verwendung. Sowohl bei BYOK als auch bei BYOE findet der eigentliche Verschlüsselungsvorgang in der Cloud statt, d.h. innerhalb von Systemen, die vom Cloud-Service-Provider verwaltet werden. Das Modell BYOE unterscheidet sich von BYOK, wo man die Kontrolle über die Schlüssel hat, durch die zusätzliche Möglichkeit, auch die verwendeten kryptografischen Algorithmen und allenfalls Funktionalitäten selbst zu verwalten. Aus Sicherheitssicht spielen diese zusätzlichen Kontrollmöglichkeiten von BYOE aber nur eine unwesentliche Rolle. **Hold Your Own Key (HYOK):** Die Verwaltungseinheit bei bleibt stets im alleinigen Besitz der Schlüssel. Diese werden idealerweise in einem Hardware Security Module (HSM) gehalten, wobei das HSM selbst auch wieder virtualisiert betrieben sein kann. In diesem Fall spricht man auch etwa von **Keep Your Own Key (KYOK),** d.h. die Organisation verfügt über die alleinige Kontrolle des virtualisierten und sich selbst auch in der Cloud befindlichen HSM.[134] Dementsprechend wird das eigene Schlüsselmaterial nicht zur Cloud übertragen. Das Ziel dieses Modells besteht darin zu verhindern, dass die Daten jemals im Klartext in die Cloud gelangen. Eine saubere Umsetzung vorausgesetzt, ist dies unbestritten ein sicheres Vorgehen zur Verhinderung ungewollter Datenzugriffe, bedeutet aber stand heute teilweise gravierende Einbussen bei der Funktionalität.
On-Premises	«On-Premises» oder On-Prem (in den eigenen Räumlichkeiten, vor Ort oder lokal) bezeichnet ein Nutzungs- und Lizenzmodell für serverbasierte Computerprogramme (Software).
Cloud-Service-Provider	Repräsentiert eine Entität, welche eine Geschäftsbeziehung mit einem Cloud-Consumer eingeht und dieser einen Service anbietet, welcher in einem Rechenzentrum läuft, das unter der Kontrolle des Cloud-Service-Providers liegt.
Cloud Cloud-Dienste Cloud-Lösungen	Die Cloud ist per se kein klarer Begriff und wird unterschiedlich interpretiert. Die meisten Interpretationen lassen sich mit on-demand Skalierbarkeit, Hochverfügbarkeit und gemeinsame Ressourcennutzung, sicheren Zugriff und gemessene Servicevereinbarungen zusammenfassen. Obwohl einige dieser Vorteile bereits gut realisierbar sind, bleiben viele Aufgabenstellungen, vor allem im Bereich der Sicherheit, im Status der laufenden Weiterentwicklung.
Mitigierungsmassnahmen	Massnahmen zur Minimierung von Risiken.
Cloud-Nutzer	Anwender von Cloud-Diensten
Unterauftragnehmer	Bei einem Unterauftragnehmer handelt es sich um einen eigenständigen Unternehmer, der von einem Generalunternehmer (auch: vorgelagertes Hauptunternehmen) Aufträge erhält. Die Bedingungen sind mit dem beauftragenden Unternehmen vertraglich zu vereinbaren, und zwar in einem Werk- oder

[134] cloud-computing-2021-11-08.pdf.

	Dienstvertrag. Unterauftragnehmer sind vor allem in den Segmenten Handwerk und Dienstleistung anzutreffen. Als Synonym kann auch Subunternehmer verwendet werden.
Service-Anbieter, Service-Provider	Entität, welche eine bestimmte Dienstleistung anbietet, und dabei ggf. auf Cloud-Anbieter (im Sinn von Unterauftragnehmern) zurückgreift.
Services	Wird gleichbedeutend mit «Dienstleistungen» verwendet.