



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

---

Bern, März 2025

---

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

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

---

## Änderungsverzeichnis

Version	Datum	Änderung	Name
0.1		Entwurf 1. Arbeitsgruppensitzung <sup>1</sup>	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 LauxLawyers 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
1.5	April 2024	Aktualisierung des Berichts	Ronja Lichtsteiner / Stephan Brunner
1.7	Oktober 2024	Überarbeitung nach Rückmeldung BJ	Ronja Lichtsteiner / Stephan Brunner
1.8	November 2024	Letzte Überarbeitungen vor ÄK	Ronja Lichtsteiner / Stephan Brunner
2.0	März 2025	Bereinigung nach ÄK	Stephan Brunner

<sup>1</sup> In der Arbeitsgruppe waren 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

<b>Teil 1 – Vorbemerkungen</b> .....	<b>7</b>
<b>1 Einleitung</b> .....	<b>7</b>
1.1 <b>Gegenstand und Adressatenkreis</b> .....	<b>7</b>
1.2 <b>Zweck des Berichts</b> .....	<b>7</b>
<b>2 Begrifflichkeiten: Cloud-Modelle und -Services</b> .....	<b>7</b>
2.1 <b>Cloud-Deployment-Modelle</b> .....	<b>8</b>
2.2 <b>Cloud-Service-Modelle</b> .....	<b>8</b>
<b>3 Risikoaspekte</b> .....	<b>9</b>
3.1 <b>Risikoevaluation- und Bewertung</b> .....	<b>10</b>
3.2 <b>Risikoakzeptanz</b> .....	<b>10</b>
<b>4 Vertragliche Vereinbarungen mit Cloud-Dienstleistern</b> .....	<b>11</b>
<b>Teil 2 – Rechtliche Rahmenbedingungen</b> .....	<b>12</b>
<b>1 Datenschutzgesetzgebung des Bundes</b> .....	<b>12</b>
1.1 <b>Personendaten und Datenbearbeitung</b> .....	<b>12</b>
1.1.1 <b>Begriff der Personendaten</b> .....	<b>12</b>
1.1.2 <b>«Bearbeiten von Personendaten»</b> .....	<b>13</b>
1.1.2.1 <b>Definition «Bearbeiten»</b> .....	<b>13</b>
1.1.2.2 <b>Voraussetzungen für das Bearbeiten von Personendaten</b> .....	<b>13</b>
1.1.3 <b>«Daten juristischer Personen»</b> .....	<b>13</b>
1.2 <b>Technische Ansätze zum Schutz der Daten</b> .....	<b>14</b>
1.2.1 <b>Anonymisierung und Pseudonymisierung von Daten</b> .....	<b>14</b>
1.2.2 <b>Verschlüsselung</b> .....	<b>15</b>
1.3 <b>Datensicherheit</b> .....	<b>17</b>
1.3.1 <b>Grundsätze</b> .....	<b>17</b>
1.3.2 <b>Bearbeitungsreglement</b> .....	<b>17</b>
1.4 <b>Vor der Nutzung eines Cloud-Services: Allfällige Datenschutz-Folgenabschätzung</b> ...	<b>18</b>
1.5 <b>Findet mit der Nutzung eines Cloud-Services eine Datenbearbeitung durch einen Auftragsbearbeiter statt?</b> .....	<b>19</b>
1.5.1 <b>Auftragsdatenbearbeitung im DSGVO</b> .....	<b>19</b>
1.5.2 <b>Auftragsdatenbearbeitung im Cloud-Kontext</b> .....	<b>20</b>
1.5.3 <b>Beizug von Unterauftragnehmern durch den Cloud-Service-Anbieter</b> .....	<b>20</b>
1.6 <b>Datenbekanntgabe ins Ausland</b> .....	<b>20</b>
1.6.1 <b>Grundsätze</b> .....	<b>20</b>
1.6.2 <b>Im Cloud-Kontext</b> .....	<b>21</b>
1.7 <b>Behördenzugriffe im Ausland</b> .....	<b>21</b>
1.7.1 <b>Rechtslage EU-Mitgliedstaaten</b> .....	<b>23</b>
1.7.2 <b>Rechtslage USA</b> .....	<b>23</b>
1.7.3 <b>Rechtslage China</b> .....	<b>25</b>
1.7.4 <b>Allgemeine weitere (politische) Risiken bei Cloud-Lösungen im Ausland</b> .....	<b>25</b>
1.8 <b>Rechte der Betroffenen</b> .....	<b>26</b>
1.8.1 <b>Grundsatz</b> .....	<b>26</b>
1.8.2 <b>Im Cloud-Kontext</b> .....	<b>26</b>
<b>2 Amtsgeheimnis</b> .....	<b>26</b>
2.1 <b>Allgemeine Bemerkungen</b> .....	<b>26</b>
2.2 <b>Der Tatbestand der Amtsgeheimnisverletzung (Art. 320 StGB)</b> .....	<b>27</b>

2.2.1	Tatbestandselemente .....	27
2.2.2	Beurteilung der Tatbestandselemente im Cloud-Kontext.....	27
2.2.2.1	Geheimnischarakter von einem Cloud-Anbieter übergebener Daten .....	27
2.2.2.2	Kenntnisnahme von den Informationen durch den Cloud-Anbieter oder Dritte («Offenbarung») .....	28
2.2.2.3	Entbindung vom Amtsgeheimnis .....	28
2.2.2.4	Hilfspersonenstatus des Cloud-Anbieters.....	28
<b>2.3</b>	<b>Schlussfolgerung .....</b>	<b>28</b>
<b>3</b>	<b>Bestimmungen zur Informationssicherheit des Bundes .....</b>	<b>29</b>
<b>3.1</b>	<b>Allgemeine Bemerkungen .....</b>	<b>29</b>
<b>3.2</b>	<b>Sicherheitsverfahren (Art. 16-19 ISG).....</b>	<b>29</b>
<b>3.3</b>	<b>Auswirkungen für Cloud-Projekte .....</b>	<b>30</b>
<b>3.4</b>	<b>Personensicherheitsprüfung (PSP) und Betriebssicherheitsverfahren (BSV).....</b>	<b>31</b>
<b>3.5</b>	<b>Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen .....</b>	<b>32</b>
3.5.1	Auswirkungen für Cloud Projekte .....	32
<b>4</b>	<b>Weitere relevante Rechtsgrundlagen .....</b>	<b>32</b>
<b>4.1</b>	<b>Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV) .....</b>	<b>32</b>
<b>4.2</b>	<b>Vorschriften zur Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen.....</b>	<b>33</b>
<b>4.3</b>	<b>Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung).....</b>	<b>34</b>
<b>4.4</b>	<b>Weisungen mit Geltung für die gesamte Bundesverwaltung .....</b>	<b>34</b>

**Anhänge<sup>2</sup>:**

- Anhang A: Literatur und Materialien
- Anhang B: Glossar
- Anhang C: Risiken und Massnahmen
- Anhang D: Checkliste

<sup>2</sup> Anstelle des bisherigen Anhang E (Übersicht Cloud-Nutzung in der Bundesverwaltung) kann auf die [Cloud-Prinzipien der Bundesverwaltung \(AR010\)](#) verwiesen werden, insb. auf Abbildung 2.

# Zusammenfassung

## Zweck des Berichts

Der Bericht soll zum einen für die Auslagerung von Daten in die Cloud 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-Auslagerungs-Projekten zu beurteilen und ihre «Compliance» zu gewährleisten. Er soll damit unter anderem auch als Basis für die Rechtsgrundlagenanalyse<sup>3</sup> bei Cloud-Auslagerungs-Projekten dienen können. Der Bericht stützt sich auf die Cloud-Strategie der Bundesverwaltung, seine Schlussfolgerungen gelten jedoch grundsätzlich auch für jedes andere IT-Outsourcing-Projekt.

## Risikoaspekte (vgl. Teil 1, Ziff. 3 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-Auslagerungs-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-Dienstleister (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-Auslagerungs-Lösungen können zu erheblichen Abhängigkeiten von einzelnen Dienstleistern führen, insbesondere was die Verfügbarkeit der Leistungen betrifft.

Welche Restrisiken<sup>4</sup> – 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<sup>5</sup> 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, Ziff. 1 Datenschutzgesetzgebung des Bundes)*

Die Datenschutzgesetzgebung erlaubt die vertraglich vereinbarte Auftragsdatenbearbeitung durch verwaltungsexterne Dritte. Soweit Auftragnehmende weitere Unterauftragnehmer beziehen, ist durch entsprechende Vertragsgestaltung und allenfalls auch technische Massnahmen durch die Auftraggebenden sicherzustellen, dass diese an die gleichen Regelungen gebunden sind, wie der Cloud-Dienstleister 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 beispielsweise 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 Auftragnehmenden 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

<sup>3</sup> Eine Vorlage zur Rechtsgrundlagenanalyse findet sich hier: [Rechtsgrundlagenanalyse erarbeiten - Aufgaben - Projektmanagement - HERMES Online](#)

<sup>4</sup> Eine Auseinandersetzung zu den Restrisiken findet sich etwa in folgender, für den Kanton Bern erstellten Analyse: KAIO, Restrisiken beim Einsatz von M 365.

<sup>5</sup> Wo keine Differenzierung aufgrund des Gesetzes nötig wird, werden Daten und Informationen als Synonyme verwendet.

verschaffen können. 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. Mit der Änderung von Anhang 1 DSV wurde die USA für Datenbekanntgaben im Rahmen des *Swiss-U.S. Data Privacy Frameworks* am 15. September 2024 in die Liste der Staaten, Gebiete spezifische Sektoren und internationale Organe mit einem angemessenen Datenschutz aufgenommen. 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-Auslagerungs-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 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, Ziff. 2 Amtsgeheimnis)*

Cloud-Anbieter sind in Artikel 320 Ziffer 1 StGB 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-Anbieter weitgehend zu verhindern, namentlich durch Verschlüsselung oder Pseudonymisierung und Tokenisierung von Daten (vgl. Teil 2, Ziff. 0).

Als Geheimnis gilt jede Tatsache, die weder offenkundig noch allgemein zugänglich ist (relative Unbekanntheit) und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat («materielles Geheimnis»; z.B. Informationen, die dem Geschäftsgeheimnis nach Art. 162 StGB oder dem Berufsgeheimnis gemäss Art. 321 StGB unterstehen). Strafbar ist die Verletzung des Amtsgeheimnisses, wenn solche Informationen durch den Geheimnisträger einem Dritten zugänglich gemacht werden, für welchen sie nicht bestimmt sind. 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 unterstellte) Cloud-Dienstleister seinerseits Daten, die unter das Amtsgeheimnis fallen, einem nicht berechtigten Dritten offenbart. Dafür müsste der Cloud-Anbieter in der Regel technische Massnahmen umgehen und er würde die vereinbarten vertraglichen Verpflichtungen verletzen sowie allenfalls gegen strafrechtliche Bestimmungen verstossen.

### *Informationssicherheit (vgl. Teil 2, Ziff. 3 Bestimmungen zur Informationssicherheit des Bundes)*

Auch die geltenden Regeln zur Informationssicherheit stehen einer Cloud-Auslagerung nicht entgegen. Daten bis und mit Klassifizierungsstufe VERTRAULICH können grundsätzlich durch Auftragnehmer in der Cloud bearbeitet werden, wenn angemessene Massnahmen zum Schutz der Informationen getroffen werden. Vorbehalten sind Weisungen, die restriktiver formuliert sind<sup>6</sup>. Gegebenenfalls sind besondere Anforderungen zu beachten (wie z.B. die Erforderlichkeit eines Betriebssicherheitsverfahrens).

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

<sup>6</sup> So namentlich die [E031 – Einsatzrichtlinie Microsoft 365](#), Ziff. 2.2 und Anhang A

# Teil 1 – Vorbemerkungen

## 1 Einleitung

### 1.1 Gegenstand und Adressatenkreis

Am 11. Dezember 2020 hat der Bundesrat die Cloud-Strategie der Bundesverwaltung verabschiedet, welche zum Ziel hat, die Nutzung von Cloud-Diensten in der Bundesverwaltung breit zu fördern.<sup>7</sup> 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:

*«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, VPSP, RVOG, ISG, DSG, Strafgesetzbuch, BGÖ), Verordnungen (z. B. ISV) und IKT-Weisungen aber auch ausländische Rechtsnormen (wie z. B. DSGVO, US CLOUD Act oder Foreign Intelligence Surveillance Act (FISA)). Dazu gehören auch Geheimhaltungspflichten (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, die mit Bezug auf Cloud-Projekte auch für die Berücksichtigung der rechtlichen Aspekte zuständig sind, sowie an Personen mit Beratungs- und Kontrollfunktionen<sup>8</sup>.

### 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, der Informationssicherheit 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-Auslagerungs-Projekten zu gewährleisten. Der Anhang C dieses Berichts enthält eine Liste mit Risiken, die bei der Auslagerung in die Cloud vorkommen können und die möglichen Massnahmen, um diese Risiken auf ein akzeptables Niveau zu senken. Diese sollen den einzelnen Verwaltungseinheiten strukturiert aufzeigen, was 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-Auslagerungs-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 herkömmliche Auslagerung.<sup>9</sup> Auch die Strategie Rechenzentren der zivilen Bundesverwaltung (RZ-Strategie) geht davon aus, dass IT-Leistungen vermehrt extern, in Public Clouds, erbracht werden.<sup>10</sup>

<sup>7</sup> Siehe [Cloud-Strategie der Bundesverwaltung \(admin.ch\)](#).

<sup>8</sup> Insbesondere die Informationssicherheitsbeauftragten sowie die Datenschutzberaterinnen und -berater.

<sup>9</sup> Siehe [Cloud-Strategie der Bundesverwaltung \(admin.ch\)](#).

<sup>10</sup> RZ-Strategie (in Erarbeitung), S. 2.

Heute bestehen auf dem Markt vier Haupttypen von Cloud-Deployment-Modellen<sup>11</sup> und drei Arten von Cloud-Service-Modellen.

Die Cloud-Deployment-Modelle lassen sich unterscheiden in:

- Public-Clouds,
- Private-Clouds,
- Hybrid-Clouds und
- Community-Clouds

Die drei Cloud-Service-Modelle 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

### *Public-Clouds*

Die Cloud-Infrastruktur wird zur offenen Nutzung durch die Allgemeinheit vom Cloud-Dienstleister 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.<sup>12</sup>

### *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 (Cloud-Dienstleister) oder einer Kombination aus beiden befinden und von diesen verwaltet und betrieben werden, und sie kann «on-premise» oder «off-premise» existieren. Die heutige noch bestehende Atlantica-Cloud des Bundes ist eine solche Private-Cloud, sie soll durch Teile der Swiss Government Cloud (SGC) abgelöst werden.

### *Hybrid-Clouds*

Die Cloud-Infrastruktur ist eine Komposition aus zwei oder mehr verschiedenen Cloud-Infrastrukturen (private, community oder public), die eigenständigen 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 (ein Beispiel dafür ist die Swiss Government Cloud des Bundes (SGC), welche auch den Kantonen und Gemeinden zur Verfügung gestellt werden könnte).

## 2.2 Cloud-Service-Modelle<sup>13</sup>

### *IaaS (Infrastructure-as-a-Service)*

<sup>11</sup> Die Definitionen richten sich nach NIST: [NIST SP 800-145, The NIST Definition of Cloud Computing](#).

<sup>12</sup> Siehe [Magic Quadrant für Cloud-Infrastruktur und Plattform-Services \(gartner.com\)](#).

<sup>13</sup> Die Definitionen richten sich nach NIST: [NIST SP 800-145, The NIST Definition of Cloud Computing](#).

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 dienen dem Zweck, 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 die zugrundeliegende Cloud-Infrastruktur einschliesslich Netzwerk, Server, Betriebssysteme, Speicher nicht, auch nicht sogar einzelne Anwendungsfunktionen. Mögliche Ausnahme sind begrenzte benutzerspezifische Einstellungen zur Konfiguration von Anwendungen.

## 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-Anbieter sich an Verträge halten und dass sie ihre Systeme nicht zum Schaden der Cloud-Nutzer manipulieren.<sup>14</sup> 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). Insbesondere im Bereich des Datenschutzes kann die DSFA ein wichtiges Hilfsmittel darstellen (siehe unten Teil 2, Ziff. 1.4)

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.<sup>15</sup>

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 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 und Teil 2, Ziff. 1.6.).

<sup>14</sup> Die Cloud-Service Provider tun dies namentlich, indem sie sich mit entsprechenden Zertifizierungen ausweisen. Vgl. ROSENTHAL, Schweizer Banken in die Cloud.

<sup>15</sup> Allerdings sind die rechtlichen 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.

- Beizug von Unterauftragnehmer: Für die Auftrags Erfüllung 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 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-Diensten 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.<sup>16</sup>

Teilweise werden solche Risiken bei Cloud-Lösungen akzentuiert, unter Umständen aber auch gemildert (ev. besserer Schutz gegen Cyberangriffe<sup>17</sup>). Risiken können mit Cloud-Lösungen aber auch in neuer Weise hinzutreten. Jede Lösung (sowohl «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. Die Restrisiken tragen in jedem Fall die jeweiligen Risikoeigner und Führungspersonen der Verwaltungseinheiten, die für die Bearbeitung der betreffenden Daten verantwortlich (im Sinne von Art. 5 Bst. j DSGVO) sind.

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), 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.<sup>18</sup>
- 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;<sup>19</sup> 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.
- Technische Risiken: Die Exponiertheit der Managementumgebung; grössere Komplexität der (Cloud-Computing) Systeme oder die grösseren Auswirkungen von Fehlkonfigurationen

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<sup>20</sup> 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 zu treffen; Einhaltung

<sup>16</sup> Siehe [Anklage macht Ausmass des Diebstahls beim Nachrichtendienst bekannt - SWI swissinfo.ch](#), vgl. dazu auch die vom Verein Unternehmensdatenschutz (VUD) herausgegebenen FAQ zum Einsatz von Cloud-Technologien ([VUD\\_FAQ zum Einsatz von Cloud.pdf](#)).

<sup>17</sup> Ob das für ein konkretes Vorhaben gilt, ist im konkreten Fall zu prüfen. A.M. Blonski Dominika, in: [Cloud – alles Risiko?](#) SJZ 119/2023 S. 991.

<sup>18</sup> So ist z.B. für Public-Cloud-Lösungen unter WTO 20007 in diesem Zusammenhang insbesondere zu beachten, dass die Rahmenverträge für eine Zeitdauer von 5 Jahren gelten, also noch bis 2026.

<sup>19</sup> Bisweilen wird dabei von «lawful access» gesprochen.

<sup>20</sup> Eine Auseinandersetzung zu den Restrisiken finden sich bei der folgenden, für den Kanton Bern erstellten Analyse: KAIO, Restrisiken beim Einsatz von M 365.

des geltenden Rechts vorausgesetzt. Die Analyse muss die im konkreten Anwendungsfall bestehenden Risiken ausweisen und die mitigierenden Massnahmen berücksichtigen. Weist die Risikoanalyse trotz Massnahmen noch ein hohes Risiko aus, heisst das noch nicht, dass eine Auslagerung nicht durchgeführt werden kann. Solange die Risiken evaluiert, adäquat bewertet und transparent ausgewiesen werden, kann sich eine Auslagerung trotz hoher Risiken insbesondere auch aus der datenschutzrechtlichen Sicht als zulässig erweisen, sofern die datenschutzrechtlichen Grundsätzen nach Artikel 6 DSGVO und den Anforderungen an die Datensicherheit nach den Artikeln 1-6 DSV eingehalten werden.<sup>21</sup>

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-Dienstleistern

Die verantwortlichen Stellen der Bundesverwaltung müssen die in den Standardverträgen der Cloud-Service-Anbietern angebotenen Konditionen sorgfältig daraufhin prüfen, ob diese dem erforderlichen Standard für die zu bearbeitenden Daten entsprechen. Grosse Cloud-Service-Anbieter («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):

- Hinweis zur Pflicht der Wahrung des Amtsgeheimnisses (vgl. Teil 2, Ziff. 0),
- Weisungsgemässe Bearbeitung von Daten (vgl. Teil 2, Ziff. 1.3.2 und 3),
- Zusätzliche Sicherheitsmassnahmen (vgl. Teil 2, Ziff. 1.2, 1.3 und 3),
- Kontrollbefugnisse, insbesondere betr. Auditergebnisse (vgl. Teil 2, Ziff. 1.3.2 und 3).

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.

---

<sup>21</sup> Siehe LOBSIGER, S. 311 ff.

## 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.<sup>22</sup> 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.<sup>23</sup> Je nach Sachbereich oder Natur der bearbeiteten Daten gelten jedoch spezifischere Anforderungen an die Rechtsgrundlage. Das gilt namentlich dann, wenn Personendaten Gegenstand einer Auslagerung in die Cloud 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. 2.2) bearbeitet werden sollen, sind die Vorgaben der Datenschutzgesetzgebung einzuhalten.

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 Ordnungsrecht 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 DSG 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. 7 DSG).

#### 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 DSG). Daten, welche diese Definition erfüllen, dürfen nur unter Einhaltung der datenschutzrechtlichen Vorgaben bearbeitet werden. Insbesondere ist für Bundesorgane eine entsprechende Rechtsgrundlage erforderlich (Art. 34 DSG).

<sup>22</sup> HÄFELIN/MÜLLER/UHLMANN, Rz 1384; TSCHANNEN/ZIMMERLI/MÜLLER, Para. 4 Rz. 8 ff.

<sup>23</sup> 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., S. 554).

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 DSG). 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.

Eine Grundlage in einem Bundesgesetz ist ebenfalls für das *Profiling* erforderlich (vgl. Art. 34 Abs. 2 Bst. b DSG) vor. Darunter fällt «jede Art der automatisierten Bearbeitung von Personendaten,<sup>24</sup> 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 DSG).

*Profiling mit hohem Risiko* ist ein Profiling, dass 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 DSG).

## 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 DSG).<sup>25</sup>

### 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 2, Ziff. 1.1.1).

Ein *Profiling* ist für Verwaltungseinheiten grundsätzlich nur gestützt auf eine formell gesetzliche Grundlage (Art. 34 Abs. 2 Bst. b DSG) erlaubt (vgl. auch oben Teil 2, Ziff. 1.1.1). Gesetz im formellen Sinne heisst für das Bundesrecht, dass die entsprechende Rechtsgrundlage auf Stufe Bundesgesetz verankert sein muss; eine Verordnung reicht nicht aus. Auch an die Normdichte sind höhere 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

## 1.1.3 «Daten juristischer Personen»

Rechtsgrundlagen für den Umgang mit Daten juristischer Personen finden sich in Artikeln 57r ff. Regierungs- und Verwaltungsorganisationsgesetz (RVOG; SR 172.010). 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 RVOG). 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.

<sup>24</sup> Siehe zum Begriff der automatisierten Bearbeitung von Personendaten: [Fragen und Antworten zum Datenschutz \(BJ\)](#).

<sup>25</sup> Zur Bearbeitung durch Cloud-Dienstleister vgl. Teil 2, Ziff. 1.5.

Artikel 57r Absatz 2 RVOG 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 RVOG). 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.<sup>26</sup>

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<sup>27</sup>) zu prüfen.<sup>28</sup>

Artikel 71 DSGVO sieht vor, dass Vorschriften in anderen Bundeserlassen, die sich auf Personendaten beziehen, für Bundesorgane während fünf Jahren nach Inkrafttreten des DSGVO weiter Anwendung auf Daten juristischer Personen finden. Insbesondere können Bundesorgane in dieser Zeit Daten juristischer Personen nach Artikel 57s Absätze 1 und 2 RVOG weiterhin bekanntgeben, wenn sie gestützt auf eine Rechtsgrundlage zur Bekanntgabe von Personendaten ermächtigt sind. Aktuell laufen die Arbeiten an einem Rechtsetzungsprojekt, mit welchem diese Übergangsbestimmung abgelöst werden soll.

## 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 Dritte mit analytischen Methoden auch bei vordergründig anonymen Daten unter Umständen einen Personenbezug wiederherstellen können.<sup>29</sup> 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, dass einzelne Elemente von Datensätzen durch Platzhalter ersetzt werden, z.B. Namen durch Nummern (ähnlich auch das Verfahren der «Tokenisierung»<sup>30</sup>). 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 lediglich dann ausreichend, wenn aufgrund der Umstände das Risiko als minimal erscheint,

<sup>26</sup> 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 (Botschaft Totalrevision DSGVO, Ziff. 3.2.3). Allerdings wird eine Cloud-Lösung und die damit verbundene Bekanntgabe in der Regel kaum «unentbehrlich» sein. Die in Artikel 57s RVOG weiter vorgesehenen Ausnahmen und Spezialfälle betreffen Bekanntgaben im Einzelfall und können für Cloud-Lösungen kaum Anwendung finden.

<sup>27</sup> 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>.

<sup>28</sup> Es ist offensichtlich vergessen worden, Art. 9 DSGVO 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 DSGVO. 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.

<sup>29</sup> Vgl. dazu GA WIDMER, S. 9 f.

<sup>30</sup> Vgl. MILLARD, S. 38.

dass Dritte, welche nicht über die entsprechenden Informationen zu Wiederherstellung des Personenbezuges verfügen, in der Lage sind, mit einem vernünftigerweise erwartbaren Aufwand<sup>31</sup> die Daten wieder Personen zuzuordnen. In diesem Fall finden die Bestimmungen des DSGVO gegenüber Dritten keine Anwendung.<sup>32</sup>

Bei der Tokenisierung handelt sich um einen Prozess, bei dem 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. Von einem Token kann nicht auf die ursprünglichen Daten geschlossen werden. Im Gegensatz zur Verschlüsselung werden bei der Tokenisierung keine kryptografische Methode zur Umwandlung von Daten in eine verschlüsselte Form (Chiffre) verwendet. Die Tokenisierung wird insbesondere bei sicheren Zahlungssystemen verwendet.

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-Dienstleister kein Rückschluss auf eine konkrete Person mehr gezogen werden kann).

## 1.2.2 Verschlüsselung

Bei der *Verschlüsselung* 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. Zentral ist dabei das Schlüsselmanagement, welches hohe Gewähr dafür bieten muss, 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*), 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-Dienstleister, Cloud-Hoster, weitere Dienstleistende; vgl. Teil 2, Ziff. 1.2.2) keinen oder nur sehr eingeschränkten Zugriff auf die Schlüssel haben. Dabei können beispielsweise folgende Ansätze gewählt werden:

- *Double Key Encryption*: Dieser Ansatz besteht darin, Daten vor der Speicherung zu verschlüsseln und dem Anbieter keinen Zugriff auf die Schlüssel zu gewähren. Da der Kunde die Schlüssel besitzt – idealerweise in einem Hardware Security Module (HSM) gespeichert –, kann der Anbieter die Daten nicht lesen. Werden Daten in der Cloud verarbeitet, entschlüsselt der Kunde sie für die Verarbeitung und verschlüsselt sie danach erneut.<sup>33</sup>
- *Externe Schlüsselverwaltungslösung*: Externe Schlüsselverwaltungslösungen erhöhen die Datensicherheit, indem sie Verschlüsselung ermöglichen, ohne die Kontrolle über die Schlüssel an den Cloud-Anbieter abzugeben. Durch die Einrichtung eines sicheren Proxys zwischen der Cloud-Umgebung und externen Schlüsselmanagern können Organisationen Datenhoheit bewahren und gleichzeitig die Skalierbarkeit und Agilität der Cloud nutzen. Für diese Systeme wird empfohlen, HSMs zu verwenden, um geheime Schlüssel sicher zu speichern. Diese HSMs sollten in Clustern an verschiedenen Standorten eingerichtet werden, um Geo-Redundanz und redundante Internetanbindung zu gewährleisten.

<sup>31</sup> 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.

<sup>32</sup> Vgl. dazu GA WIDMER, S. 10.

<sup>33</sup> Für Microsoft Office-Anwendungen kann DKE – Double Key Encryption verwendet werden. Damit können Office-Dokumente und E-Mails auf dem Computer verschlüsselt werden, bevor sie in die Azure Cloud gelangen.

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 Verschlüsselungsstandards sowie die Massnahmen zum Schutz der Schlüssel für den jeweiligen Zweck ausreichend sind.<sup>34</sup> 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 neuere Schweizer Technologie, die eine sichere Datenübertragung (Routing) automatisiert gewährleisten soll.<sup>35</sup> 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.<sup>36</sup>

### *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 unbefugtem 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»<sup>37</sup>). Eine neue Technik ist das Confidential Computing, das es den Cloud-Dienstleistern verunmöglicht auf Daten während der Bearbeitung zuzugreifen.<sup>38</sup>

Nach heutigem Stand der Technik ist das Risiko des Datenzugriffs durch Unbefugte bei *data in use* in der Regel am ehesten gegeben.<sup>39</sup> 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). Zukünftige Systeme mit «voll homomorpher» Kryptografie<sup>40</sup> werden allenfalls die Möglichkeit bieten, Daten zu bearbeiten, ohne sie zu entschlüsseln.

<sup>34</sup> 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.

<sup>35</sup> Nur Gateway to Gateway, Broad Network Access ist zurzeit nicht unterstützt, da Endgeräte nicht z.B. mittels eines SCION Agents unterstützt werden. Weiterführende Informationen zu SCION: [SCION Internet Architecture \(scion-architecture.net\)](https://scion-architecture.net).

<sup>36</sup> Auch neue Ansätze wie Secure Access Service Edge (SASE) können eingesetzt werden, inkl. Zero Trust Network Access (ZTNA). Vgl. auch MILLARD, S. 38.

<sup>37</sup> MILLARD, S. 39 f.

<sup>38</sup> Vgl. [BACS - Technologiebetrachtung: Confidential Computing](#).

<sup>39</sup> Soweit Data at rest und in transit verschlüsselt sind und der CSP nicht ohne Weiteres Zugriff auf die Schlüssel hat.

<sup>40</sup> Siehe zur Definition und weiteren Erklärungen: [Homomorphe Verschlüsselung – Wikipedia](#)

## 1.3 Datensicherheit

### 1.3.1 Grundsätze

Artikel 8 DSGVO 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<sup>41</sup>.

Die Verordnung zum Datenschutzgesetz gibt Grundsätze vor betreffend:<sup>42</sup>

- Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit);
- 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, Ziff. 3 und 4 insbesondere im [Informationssicherheitsgesetz \[ISG\]](#)<sup>43</sup> und der dazugehörigen [Informationssicherheitsverordnung \[ISV\]](#)<sup>44</sup>). Auch einige Weisungen regeln Sicherheitsaspekte, etwa beim Einsatz von Mobilgeräten oder zum IT-Grundschutz.<sup>45</sup>

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

### 1.3.2 Bearbeitungsreglement

Die Massnahmen sind in einem Bearbeitungsreglement<sup>46</sup> (Art. 5 i.V.m. Art. 6 Abs. DSV) detailliert zu regeln. Dieses Bearbeitungsreglement ist dann zu erstellen, wenn die Voraussetzungen von Artikel 6 Absatz 1 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 oft aus einem Service-Katalog ausgewählt werden (von der Auswahl sind dann die Lizenzen und deren 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<sup>47</sup> vorzusehen sind (einschliesslich Haftungsregelungen bzw. Konventionalstrafen; vgl. zum Ganzen auch Anhang C):

- 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 DSGVO).<sup>48</sup>
- Unklare organisatorische Regelungen im Umfeld der Shared Responsibility: Klare AKV (Aufgaben, Kompetenzen, Verantwortung) müssen vereinbart werden, auch im Umfeld der Cloud Security (z.B. Interaktionen mit dem Cloud-Dienstleister Security Operations Center [SOC]).

<sup>41</sup> Vgl. auch die AR010 Ziff. 4.2.2 (Sicherheitsverfahren durchführen).

<sup>42</sup> Vgl. auch den [Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes vom 15. Januar 2024](#); sowie GA WIDMER, S. 15.

<sup>43</sup> SR 128

<sup>44</sup> SR 128.1

<sup>45</sup> [BACS Si001](#), und [E026 - Einsatzrichtlinie Arbeitsplatzsystem](#), insbes. 2.3 – 2.5.

<sup>46</sup> Vgl. [EDÖB. Häufige Fragen zum Datenschutz. Stichwort Bearbeitungsreglement](#).

<sup>47</sup> 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.

<sup>48</sup> In der Ausschreibung zur WTO 20007 wurde dieser Aspekt in Ziff. 8.1 bereits definiert.

- Bearbeitung von Daten auf gemeinsam mit «fremden» Dienstleistungsbeziehenden genutzten Infrastrukturen und dadurch insbesondere erhöhtem Risiko eines Versagens der Datenisolation bei einer bloss logischen statt physischer Trennung: Physisch getrennte Infrastrukturen vereinbaren; besondere Architekturmodelle.
- Unbefugte Dritte erhalten Zugang zu Daten: 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<sup>49</sup>, 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 DSG muss der Verantwortliche 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 DSG beispielsweise die Verwendung neuer Technologien sowie 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 DSG). Bleibt trotz der getroffenen oder geplanten Massnahmen ein hohes «Restrisiko» für die Persönlichkeit oder die Grundrechte der betroffenen Person bestehen, muss der EDÖB<sup>50</sup> konsultiert werden (Art. 23 Abs. 1 DSG).<sup>51</sup>

Der Bundesrat hat für die Bundesverwaltung eine Richtlinie für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen<sup>52</sup> erstellt, welche eingehalten werden muss. Die Richtlinie regelt im Wesentlichen die Durchführung der Risikovorprüfung und der DSFA und deren Einbettung in das Rechtsetzungsverfahren des Bundes sowie die Koordination mit der Projektmanagementmethode HERMES. Des Weiteren hat das Bundesamt für Justiz (BJ) ein Instrument zur Risikovorprüfung entwickelt.<sup>53</sup> Diese Risikovorprüfung soll feststellen, ob eine DSFA erforderlich ist und soll bei jeder geplanten Bearbeitung von Personendaten durchgeführt werden. Stellt die Risikovorprüfung fest, dass ein hohes Risiko für die Grundrechte der betroffenen Personen besteht, muss eine DSFA erstellt werden. Auch hat das BJ einen DSFA-Leitfaden erstellt, der Informationen zur Durchführung der DSFA enthält.<sup>54</sup>

<sup>49</sup> Vgl. auch AR010, Ziff. 4.1.3: Verpflichtung zur Definition einer Exit-Strategie.

<sup>50</sup> Der EDÖB hat auf seiner Website Informationen sowie ein Merkblatt zur Datenschutz-Folgenabschätzung aufgeschaltet: [Datenschutz-Folgenabschätzung \(admin.ch\)](#).

<sup>51</sup> Ein hohes «Restrisiko» bedeutet nicht, dass die Daten nicht in die Cloud ausgelagert werden dürfen. Siehe dazu auch LOBSIGER, S. 311 ff.

<sup>52</sup> BBl 2023 1882 ([Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung | Fedlex \(admin.ch\)](#)).

<sup>53</sup> Siehe [Informationen für Bundesorgane \(admin.ch\)](#).

<sup>54</sup> Siehe [BJ, DSFA-Leitfaden](#).

In Bezug auf Cloud-Projekte bedeutet dies, dass mittels einer Risikoprüfung und 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, wobei ein hohes Risiko einer Auslagerung der Daten in die Cloud nicht per se im Weg steht, sofern sie mit den Grundsätzen des Datenschutzes vereinbar und die Datensicherheit sichergestellt ist (siehe dazu auch vorne Teil 2, Ziff. 1.4).<sup>55</sup>

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

### 1.5.1 Auftragsdatenbearbeitung im DSGVO

Artikel 9 DSGVO 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.<sup>56</sup> Der Auftragsbearbeiter darf insbesondere Daten nicht zu eigenen Zwecken bearbeiten.<sup>57</sup> 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 DSGVO). 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 DSGVO). Diese kann auch vorgängig beispielsweise im Vertrag mit dem Cloud-Dienstleister erteilt werden. In diesem Fall sollte der Bundesstelle ein Widerspruchsrecht eingeräumt werden, mit dem sie solche Unterauftragsbeziehungen ablehnen kann. Solche Unterauftragsbearbeiter werden durch Cloud-Dienstleister häufig eingesetzt (z.B. für das physische Aufbewahren der Daten, für Netzwerkdienstleistungen und/oder für Unterhalt und Wartung; vgl. unten Teil 2, Ziff. 1.5.3).

Zusätzlich zum Datenschutzgesetz regelt Artikel 12 der Digitalisierungsverordnung (DigiV; SR 172.010.58) das Zugänglichmachen von Daten für externe Leistungserbringer.<sup>58</sup> 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 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.

<sup>55</sup> LOBSIGER, S. 311 ff.

<sup>56</sup> Vgl. dazu z.B. BAERISWYL, Rz. 30 ff.

<sup>57</sup> 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.

<sup>58</sup> Bei dieser Bestimmung geht es eigentlich nicht um den Daten- sondern um den Geheimnisschutz, vgl. unten Teil 2, Ziff. 2.2.

## 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. 2.2). In der Regel wird der Cloudanbieter die Auftragsbearbeitung zumindest sehr beschränkt wahrnehmen, weil er nur in ganz bestimmten und im Voraus vereinbarten Einzelfällen auf die Daten zugreifen kann.

Auch wenn Cloudanbieter nicht auf die Daten selber zugreifen können, so sind sie gemäss Auslagerungsvertrag dennoch für die Gewährleistung der Einhaltung der datenschutzrechtlichen Anforderungen und der Datensicherheit zuständig.

## 1.5.3 Beizug von Unterauftragnehmern durch den Cloud-Service-Anbieter

Für die Erfüllung seiner Aufgaben wird der Cloud-Anbieter regelmässig auf Unterauftragnehmer zurückgreifen. Diese nehmen oft Kernfunktionen wahr, sei es beim physischen Hosting der Daten (Cloud Hosting Cloud-Anbieter), 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 DSGVO und 12 DigiV). Dies muss zwingend vertraglich so festgehalten werden. Gegebenenfalls sind zusätzliche Massnahmen nötig.<sup>59</sup>

## 1.6 Datenbekanntgabe ins Ausland

### 1.6.1 Grundsätze

Artikel 16 ff. DSGVO 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 DSGVO).<sup>60</sup> Diese Staaten werden in einer Liste im Anhang 1 der DSV aufgeführt. Aktuell erfüllen namentlich die Mitgliedstaaten der EU, UK, USA im Rahmen des *Swiss-U.S. Data Privacy Frameworks*, Argentinien und Neuseeland diese Anforderungen, im Gegensatz bspw. zu China.

Ist eine Datenbekanntgabe in einen 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<sup>61</sup> oder spezifischer Garantien, die die zuständige Verwaltungseinheit erarbeitet und dem EDÖB vorgängig mitgeteilt hat.<sup>62</sup> Zudem sind auch angemessene technische und organisatorische Massnahmen zu treffen, z.B. namentlich eine Verschlüsselung der Daten, welche den Zugriff auf die Personendaten durch den (ausländischen) Auftragsdatenbearbeiter und allfällige Unterauftragnehmer weitgehend ausschliesst.<sup>63</sup> Allenfalls ist zu prüfen, ob Vorgaben für «data in transit» möglich sind, z.B. betreffend das Routing<sup>64</sup> (vgl. Teil 2, Ziff. 1.2.2).

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 DSGVO). Indessen ist darauf hinzuweisen, dass Einwilligungslösungen für systematische Datenbearbeitungen aufgrund der hohen entsprechenden Anforderungen (vgl. Art. 6 Abs. 6 und 7 DSGVO) keine geeignete Lösung ist.

Weiter zu berücksichtigen ist, dass in solchen Fällen die besondere Informationspflicht nach Artikel 19 Absatz 4 DSGVO greifen kann, wenn Daten ins Ausland bekannt gegeben werden und im Empfangsstaat

<sup>59</sup> vgl. [EDÖB – Auftragsdatenbearbeitung](#).

<sup>60</sup> 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 DSGVO).

<sup>61</sup> vgl. [EDÖB – Bekanntgabe von Personendaten ins Ausland](#). Im Rahmen der Ausschreibung WTO 20007 war eine entsprechende Anforderung vorgesehen; vgl. Anforderungskatalog, S. 12 (ZK03)

<sup>62</sup> Vgl. dazu [EDÖB – Bekanntgabe von Personendaten ins Ausland](#).

<sup>63</sup> 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.

<sup>64</sup> So ist etwa eine Verpflichtung zur Nutzung des SCION-Standards denkbar.

keine angemessene Datenschutzgesetzgebung besteht. Soweit die Bearbeitung nicht gesetzlich vorgesehen ist (Art. 20 Abs. 1 Bst. b DSGVO; was allerdings für Behörden ohnehin eine allgemeine Voraussetzung ist) müssen die Betroffenen über den Empfangsstaat und ggf. die Garantien nach Artikel 16 Absatz 2 DSGVO informiert werden. Ausnahme davon bilden Artikel 20 Absatz 2 DSGVO, nämlich wenn die Information nicht möglich ist oder die Information einen unverhältnismässigen Aufwand erfordert.

## 1.6.2 Im Cloud-Kontext

Ob bei einer Auslagerung in die Cloud eine Datenbekanntgabe im Sinne des DSGVO vorliegt, ist im Einzelfall zu prüfen.<sup>65</sup> Dies ist z.B. dann grundsätzlich nicht der Fall, wenn Daten anonymisiert und verschlüsselt sind (vgl. oben Teil 2, Ziff. 1.2.2) oder wenn andere Vorkehrungen getroffen werden, um eine Kenntnisnahme vom Dateninhalt bzw. «Klartext» durch den Cloud-Anbieter auszuschliessen.

Die Cloud-Anbieter 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.<sup>66</sup>

Bei der Nutzung von Cloud-Lösungen muss sich der Cloud-Anbieter 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.<sup>67</sup> Es muss vom Cloud-Anbieter 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 diese 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.<sup>68</sup>

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.<sup>69</sup> 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 (Unverletzlichkeit gemäss dem Wiener Übereinkommen über diplomatische Beziehungen, SR 0.191.01, und dem Wiener Übereinkommen über konsularische Beziehungen, SR 0.191.02).<sup>70</sup>

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.<sup>71</sup> Wenn diesbezüglich Unsicherheiten bestehen, ist eine entsprechende Analyse sowie die Risikoprüfung zur Datenschutz-Folgenab-

<sup>65</sup> Vgl. dazu auch z.B. BAERISWYL, Rz. 31 ff., 65 ff., 75 ff.; Bühler/Rampini, Rz 38

<sup>66</sup> Vgl. für WTO 20007 Pflichtenheft Ziff. 8.1.

<sup>67</sup> Im Rahmen der Ausschreibung WTO 20007 musste eine entsprechende Anforderung zugesichert werden; vgl. Anforderungskatalog, S. 8 (TS04).

<sup>68</sup> Vgl. SUVA, S. 3 f. und 7 f. m.H.

<sup>69</sup> 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.

<sup>70</sup> Diesbezüglich bestehen Bemühungen des EDA (DV), mit relevanten Staaten ein gemeinsames Verständnis über die Unverletzlichkeit von Daten institutioneller Begünstigter (internationale Organisationen, diplomatische und konsularische Vertretungen) zu erreichen.

<sup>71</sup> Hier sind insbesondere die verfassungsmässigen Grundsätze, wie das Legalitätsprinzip (Art. 5 BV); das Verhältnismässigkeitsprinzip (Art. 5 Abs. 2 BV, Art. 4 Abs. 2 DSGVO) oder die Rechtsweggarantie und der Zugang zu einem unparteiischen Gericht (Art. 29 ff. BV und Art. 15 DSGVO) angesprochen.

schätzung durchzuführen<sup>72</sup> 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:<sup>73</sup>

- *Justizverfahren:* Im Rahmen von Justizverfahren wird regelmässig vorgesehen,<sup>74</sup> 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<sup>75</sup> (und sind n.b. auch in der Schweiz geltendes Recht<sup>76</sup>). In der Regel bestehen verfahrensmässige Sicherungen zu Gunsten von Daten, namentlich, wenn es sich um Behörden Daten 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<sup>77</sup>). Diese findet in der Regel ohne Wissen der Betroffenen und ggf. auch ohne Wissen des «Datenherrs» statt. Deren Rechte können indessen zumindest teilweise durch den Cloud-Anbieter 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<sup>78</sup> 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-Anbieter, 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.<sup>79</sup>

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 Cloud-Anbieter (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.<sup>80</sup>

Soweit damit zu rechnen ist, dass diesbezügliche Restrisiken<sup>81</sup> verbleiben könnten, sind diese nach der hier vertretenen Ansicht mit geeigneten Massnahmen auf ein akzeptables Mass zu senken.

<sup>72</sup> Ein strukturiertes Analyseinstrument, das als «gute Praxis» gelten kann, hat ROSENTHAL entwickelt: <https://www.rosenthal.ch/downloads/Rosenthal-Cloud-Lawful-Access-Risk-Assessment.xlsx>. Es wurde kürzlich um eine Version erweitert, die es erlaubt, auch das Risiko verschiedener Entwicklungsszenarien (z.B. Entwicklung der politischen und rechtlichen Rahmenbedingungen im Heimatstaat von Cloud-Anbietern bzw. ihren Muttergesellschaften) einzubeziehen und zu bewerten: [Wie in Zeiten von Trump mit US-Cloud-Risiken umgehen - VISCHER](https://vischerink.com/flara) (Blogbeitrag 23.5.2025); <https://vischerink.com/flara>.

<sup>73</sup> Für eine Darstellung der verschiedenen Formen vgl. auch ROSENTHAL, FAQ, Nr. 28.

<sup>74</sup> Vgl. insbesondere auch Art. 18 Abs. 1 Cybercrime Convention und den Stored Communications Act.

<sup>75</sup> 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.

<sup>76</sup> Vgl. zur Rechtslage betr. Behördenzugriffe in der Schweiz auch die Ausführungen bei LAUX/HOFFMANN, N 120 ff.

<sup>77</sup> Auch die Schweiz kennt Rechtsgrundlagen, welche eine verdeckte Datenbeschaffung erlauben, vgl. heute insbesondere Art. 26 Abs. 2 und 33 Nachrichtendienstgesetz; SR 121.

<sup>78</sup> Auch die Schweiz hat eine gesetzliche Grundlage für die Funk- und Kabelaufklärung, vgl. Art. 38 ff. Nachrichtendienstgesetz.

<sup>79</sup> 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. PERLROTH.

<sup>80</sup> Vgl. SUVA, S. 7 f. m.H.

<sup>81</sup> Eine Auseinandersetzung zu den Restrisiken in kantonalem Umfeld finden sich bei: KAIO, Restrisiken beim Einsatz von M 365.

## 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 DSG ableiten. Gemäss Anhang I DSV 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<sup>82</sup>) bestehen dennoch Risiken, dass es im Rahmen von Justizverfahren, zu präventiven Zwecken und im Rahmen von Auslandüberwachungsmassnahmen zu Behördenzugriffen auf Daten kommen kann. Mit Inkrafttreten des E-Evidence-Pakets werden ab Ende Juli 2026 Anbieter digitaler Dienste in der EU zudem verpflichtet, auf Anordnung einer Strafverfolgungsbehörde eines EU-Mitgliedstaats elektronische Daten direkt herauszugeben, ohne dass ein besonderes Rechtshilfeverfahren unter Einbezug der Justizbehörden durchlaufen wird<sup>83</sup>. Diese Regeln können dazu führen, dass Rechtskonflikte entstehen, da das Schweizer Recht weiterhin den Rechtshilfeweg vorsieht<sup>84</sup>.

Grundsätzlich kann indessen davon ausgegangen werden, dass in EU-Staaten keine besonderen rechtlichen Risiken bestehen und betreffend solcher Behördenzugriffe grundsätzlich 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, ob aufgrund gewisser nachrichtendienstlicher Überwachungsprogramme<sup>85</sup> («Geheimdienstzugriffe») sowie der im US CLOUD-Act vorgesehenen Möglichkeit für Strafverfolgungsbehörden, auf Daten des Bundes beim Cloud-Anbieter zugegriffen werden kann. Der US CLOUD-Act und der Foreign Intelligence Surveillance Act (FISA) werden oft als erhebliche Risiken wahrgenommen.<sup>86</sup> Diese Gesetze ermöglichen in gewissen Fällen Datenzugriffe für amerikanische Behörden, auch dann, wenn diese Daten ausserhalb der USA bearbeitet werden, namentlich von Firmen mit Sitz in den USA oder mit anderen rechtlichen Beziehungen zur USA («incorporated in the United States»)<sup>87</sup>.

Grundsätzlich fallen auch die europäischen Töchter von amerikanischen Firmen unter diese Bestimmungen (in vielen Konstellationen indessen greifen Ausnahmen<sup>88</sup>). Allerdings kann eine direkt an sie adressierte Herausgabeanordnung der US-Strafverfolgungsbehörden ausserhalb des US-Territoriums nicht mit strafprozessualen 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.

Präsident Biden unterzeichnete am 7. Oktober 2022 die Exekutivverordnung 14086<sup>89</sup> (EO 14086), welche neue Regeln und Verbindlichkeiten zur Beschränkung des Datenzugriffs durch die US-Geheimdienste enthält. Geheimdienstliche Aktivitäten unterliegen nun zusätzlichen Garantien und dürfen unter anderem nur im Rahmen definierter nationaler Sicherheitsziele durchgeführt werden. Des Weiteren

<sup>82</sup> Vgl. die Übersicht hier: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (8.8.2022).

<sup>83</sup> Vgl. BJ, Bericht e-Evidence, Ziff. 2.

<sup>84</sup> Vgl. BJ, Bericht e-Evidence, Ziff. 5. Der Bundesrat hat am 9. April 2025 das EJPD beauftragt, Sondierungsgespräche mit der EU aufzunehmen sowie die Schaffung notwendiger Gesetzesgrundlagen zu prüfen, vgl. Medienmitteilung des EJPD vom gleichen Datum, [news.admin.ch/de/nsb?id=105595](https://www.news.admin.ch/de/nsb?id=105595).

<sup>85</sup> Vgl. dazu FAQ zum Einsatz von Cloud-Technologien ([www.vud.ch/view/data/2124/Div\\_Dokumente/220826\\_VUD\\_FAQ\\_zum\\_Einsatz\\_von\\_Cloud.pdf](http://www.vud.ch/view/data/2124/Div_Dokumente/220826_VUD_FAQ_zum_Einsatz_von_Cloud.pdf)), welche den risikobasierten Ansatz explizit anerkennen.

<sup>86</sup> ROTH, S. 68; vgl. dazu auch BRAUNECK oder ROSENTHAL, US CLOUD Act und BJ, Bericht zum US CLOUD Act. SCHEFER/GLASS vertreten die Meinung, dass es sich bei der Speicherung von Personendaten in einer US-Cloud um eine Speicherung der Daten auf Vorrat handelt und es sich somit um einen faktischen und rechtlichen Kontrollverlust über die Daten handelt (siehe dazu SCHEFER/GLASS, Gutachten M365, S. 28 ff.; kritisch dazu ROSENTHAL, Anmerkungen zum Gutachten Schefer/Glass zu «M365» und LAUX/HOFMANN in: Aktennotiz zum Rechtsgutachten Schefer/Glass. Beide vertreten die gut begründete Auffassung, dass gewisse rechtliche und technische Annahmen, von denen das Gutachten ausgeht, nicht zutreffen); ähnlich auch EPINEY/FREI, Verfassungs- und völkerrechtliche Vorgaben der Bekanntgabe von Personendaten ins Ausland im Rahmen einer Auftragsbearbeitung, Oktober 2023

<sup>87</sup> D.h. Daten können grundsätzlich auch herausverlangt werden, wenn sie in der Schweiz oder in Europa liegen. Vgl. BJ, Bericht zum US CLOUD Act, S. 6, m.Hinw.a. ein Papier des US Department of Justice.

<sup>88</sup> Vgl. ROSENTHAL, FAQ, Nr. 32, 35 und 36.

<sup>89</sup> [Office of Privacy and Civil Liberties | Executive Order 14086 \(justice.gov\)](https://www.justice.gov/opa/record/2022-10-07).

ren muss die Privatsphäre aller betroffenen Personen ungeachtet ihrer Nationalität oder ihres Wohnsitzlandes geschützt werden und ein Datenzugriff darf nur dann erfolgen, wenn dies notwendig ist, um eine anerkannte nachrichtendienstliche Priorität zu verfolgen. Der Datenzugriff muss dabei stets verhältnismässig sein.

### *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 erfassten Diensteanbietern nur dann herausgegeben werden, wenn sie darüber faktische oder rechtliche Kontrolle haben.<sup>90</sup> All diese Begriffe entspringen allerdings dem US-Recht und werden von den US-Strafverfolgungsbehörden gemäss dem amerikanischen Verständnis ausgelegt. Die Cloudanbieter können die Massnahmen in bestimmten Fällen vor einem US-Gericht anfechten; es bestehen verfahrensrechtliche Sicherungen, die jedoch gemäss dem europäischen Gerichtshof keinen genügenden Rechtsschutz für die betroffenen Personen bieten.<sup>91</sup> Diesen stehen schliesslich unter dem CLOUD Act nur beschränkt Rechtsschutzmöglichkeiten gegen solche Datenzugriffe durch die amerikanischen Behörden zur Verfügung, was nicht mit den verfassungsrechtlichen Garantien der schweizerischen Bundesverfassung vereinbar ist.<sup>92</sup>

### *Nachrichtendienstliche Auslandüberwachung (FISA und Executive Order [EO] 12333) und Garantien (EO 14086)*

Der Foreign Intelligence Surveillance Act (FISA) erlaubt gewissen Behörden die Beschaffung von Informationen aus dem Ausland. Gemäss Abschnitt 702 dürfen der Attorney General und der Director of National Intelligence die Informationsbeschaffung über bestimmte Kategorien der zu erhebenden Auslandsaufklärungsdaten bewilligen. In diesen Fällen werden amerikanische Diensteanbieter verpflichtet, die bei Ihnen vorhandenen Daten zu durchsuchen.<sup>93</sup>

Gemäss Abschnitt 2 (Section 2) der EO 14086 werden neu die U.S.-Geheimdienste verpflichtet, ihre Aktivitäten auf das Notwendige und Verhältnismässige zu beschränken. Das ist eine direkte Antwort auf die Einschätzung des europäischen Gerichtshofs, dass weder Section 702 FISA noch die Executive Order 12333 – beides Rechtsgrundlagen für die Signalüberwachung der U.S.-Geheimdienste – im Einklang mit den rechtsstaatlichen und datenschutzrechtlichen Garantien im EU-Recht steht. Danach sollen die geheimdienstlichen Aktivitäten zur Signalüberwachung nur im Einklang mit spezifischen in der EO 14086 genannten Prinzipien erfolgen und nachdem auf der Grundlage einer Bewertung aller relevanten Faktoren festgestellt wurde, dass die Tätigkeiten erforderlich sind, um eine anerkannte nachrichtendienstliche Priorität zu erzielen. Die EO 14086 erklärt, was dies praktisch bedeutet und listet zwölf legitime Ziele für Nachrichtentätigkeit auf.<sup>94</sup>

Die EO 14086 weist im dritten Abschnitt (Section 3) den Attorney General (Generalstaatsanwalt) an, einen zweistufigen Rechtsmittel-Mechanismus mit einem Gericht zur Datenschutzüberprüfung (Data Protection Review Court, DPRC) einzurichten. In erster Instanz dient der Bürgerrechts- und Datenschutzbeauftragte (Civil Liberties and Privacy Officer, CLPO) des Büros des Direktors des Nationalen Nachrichtendienstes (ODNI) als Beschwerdestelle für betroffene Personen. Der CLPO soll die Beschwerden betroffener Personen untersuchen und bei Rechtsverletzungen angemessene Abhilfemassnahmen festlegen. Die Geheimdienste sind verpflichtet, den CLPO bei seinen Untersuchungen zu unterstützen und seine Anordnungen zum Schutz der Rechte der betroffenen Personen zu befolgen. Diese haben die Möglichkeit, die Entscheidung des CLPO von dem neu geschaffenen DPRC als zweite Instanz überprüfen zu lassen. Von diesem Beschwerdemechanismus können nur betroffene Personen aus Staaten profitieren, welche vom Generalstaatsanwalt als qualifiziert bezeichnet wurden, weil deren Gesetzgebung insbesondere angemessene Garantien für die Durchführung nachrichtendienstlicher Aktivitäten bieten. Die Schweiz erhielt diese Qualifikation von den USA am 7. Juni 2024.<sup>95</sup>

### *Schlussfolgerungen*

<sup>90</sup> ROSENTHAL, FAQ, Nr. 35. Gemäss dem Bericht des Bundesamtes für Justiz ist entscheidend, dass der Diensteanbieter nicht auf den Schlüssel zugreifen kann; vgl. BJ, Bericht zum US CLOUD Act., S. 45 f.

<sup>91</sup> Vgl. Z.B. ROSENTHAL, US CLOUD Act, S. 40 und FAQ, Nr. 29. Eine ausführliche Beschreibung der Abläufe findet sich bei LAUX/HOFFMANN, S. 42 ff.

<sup>92</sup> Vgl. BJ, Bericht zum US CLOUD Act, S. 35 f.

<sup>93</sup> Ausführlich dazu ROSENTHAL, FAQ, Nr. 29.

<sup>94</sup> Siehe zum ganzen Abschnitt auch: VON WALTER, S. 294 ff.

<sup>95</sup> [Attorney General Designation of Switzerland - Designation Pursuant to Section 3\(f\) of Executive Order 14086 \(justice.gov\)](https://www.justice.gov/opa/pr/2024/06/24-0001). Zu den Designations des U.S. Generalstaatsanwalts allgemein, siehe zudem [Office of Privacy and Civil Liberties | Executive Order 14086 \(justice.gov\)](https://www.privacy.gov/opa/pr/2024/06/24-0001).

Seit dem Inkrafttreten der Änderungen von Anhang 1 DSV am 15. September 2024 können Personendaten aus der Schweiz an im Rahmen des *Swiss-U.S. Data Privacy Frameworks* zertifizierte Organisationen in den USA ohne zusätzliche Garantien übermittelt werden. Die aktuellen politischen Entwicklungen in den USA werden durch die zuständigen Stellen beobachtet.

Um im Übrigen das Risiko eines Behördenzugriffs zu senken, sollte mit geeigneten technischen Massnahmen verhindert werden, dass der Cloud-Anbieter Zugriff auf die Daten erhält. Dieser kann nicht zur Entschlüsselung von Daten gezwungen werden, wenn er nicht über die Schlüssel verfügt, sondern nur der Cloud-Nutzer. Die Herausgabe von Inhaltsdaten in solchen Verfahren ist sehr selten.<sup>96</sup>

### 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-Anbieter im Ausland gespeichert werden, ohne verlässliche verfahrensrechtliche Sicherungen durch chinesische Behörden zugegriffen werden kann oder dass diese blockiert werden könnten, kann nicht ausgeschlossen werden.<sup>97</sup> Eine diesbezügliche Beurteilung scheint auch schwierig aufgrund der grossen Vielzahl von gesetzlichen Grundlagen, welche für einen Datenzugriff in Frage kommen können.<sup>98</sup>

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.<sup>99</sup>

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,<sup>100</sup> allenfalls ist sogar die Datenverschlüsselung an sich unzulässig,<sup>101</sup> jedenfalls soweit Behörden dadurch keinen Zugriff mehr hätten. Zudem verbietet das chinesische Recht grundsätzlich die Verwendung von mit VPN gesicherten Verbindungen.<sup>102</sup>

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 Aufbewahrungs-Standorte vereinbaren.
- Politischer Druck auf Cloud-Anbieter mit Blick auf Herausgabe von Daten oder Schlüsseln bzw. die Zurverfügungstellung von Nachschlüsseln (backdoors): Vorgängige Prüfung und anschliessend Beobachtung von politischen Entwicklungen.

<sup>96</sup> Vgl. z.B. LAUX/HOFFMANN, Rz. 208 ff. [Law Enforcement Request Report | Microsoft CSR](#); Vgl. ROSENTHAL, US CLOUD Act, S. 33 f.

<sup>97</sup> Vgl. auch die Hinweise bei ROSENTHAL, FAQ, Nr. 28.

<sup>98</sup> 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](https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx) (2.3.2023).

<sup>99</sup> Vgl. z.B. HILLMANN, S. 153; LI/CHEN, S. 5.

<sup>100</sup> Vgl. z.B. DICKINSON, oder CHEN/LIU, S. 4.

<sup>101</sup> BURRI, S. 264 ff.

<sup>102</sup> Vgl. z.B. NZZ, S. 23, oder CHANDER/SUN, S. 11.

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.

## 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 DSG) und der Anspruch auf Unterlassung einer nicht rechtmässigen Bearbeitung bzw. Löschung nicht rechtmässig bearbeiteter Daten (Art. 41 DSG).

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 DSG). 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 DSG.

Gemäss Artikel 41 Absatz 2 Buchstabe a DSG 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 DSG).

### 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 die 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 schützt zum einen den Bürger und seine Geheimnisse und zum anderen die Verwaltung, um eine ungehinderte Amtstätigkeit garantieren zu können. Es ist in Artikel 320 StGB verankert und für Mitarbeitende der Bundesverwaltung in Artikel 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. Art. 61 ff. Heilmittelgesetz). An dieser Stelle wird schwergewichtig die Verletzung des Amtsgeheimnisses gemäss Artikel 320 StGB im Vordergrund stehen, welcher die strafrechtlichen Konsequenzen festlegt.<sup>103</sup>

Das Öffentlichkeitsgesetz vom 17. Dezember 2004 (BGÖ; SR 152.3) spiegelt den Amtsgeheimnisbegriff und beschränkt die «Reichweite» des Amtsgeheimnisses.<sup>104</sup> 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:

<sup>103</sup> Es sei hier noch erwähnt, dass es neben Artikel 320 StGB noch weitere Strafrechtsbestimmungen relevant sein können, so z.B. Artikel 267 StGB (diplomatischer Landesverrat). Da dieser Artikel jedoch seit Jahrzehnten kaum angewandt wird, wird auf eine vertiefere Auseinandersetzung mit dieser Bestimmung zum jetzigen Zeitpunkt verzichtet.

<sup>104</sup> Vgl. BSK StGB-Oberholzer, Art. 320 N 5 und BJ/EDÖB, Ziff. 1.1.2 und 1.1.3.

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

Eine allenfalls bestehende Klassifizierung von Informationen bedeutet dabei noch nicht in jedem Fall, dass diese auch dem Amtsgeheimnis unterstehen. Vielmehr ist zu überprüfen, ob die Klassifizierung noch gerechtfertigt ist. Das gilt insbesondere für Informationen, die INTERN klassifiziert sind (vgl. Art. 13 Abs. 1 ISG sowie Teil 2, Ziff. 3.2 unten).

## 2.2 Der Tatbestand der Amtsgeheimnisverletzung (Art. 320 StGB)

### 2.2.1 Tatbestandselemente

Gemäss Artikel 320 Ziffer 1 StGB 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<sup>105</sup> sein oder eine Hilfsperson eines Beamten. Die Legaldefinition erfasst institutionelle und funktionelle Beamte.<sup>106</sup>
- 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).<sup>107</sup>
- Die Tathandlung besteht im Offenbaren des Amtsgeheimnisses. Offenbaren bedeutet, das Geheimnis einem Dritten zugänglich machen, für welchen diese Information nicht bestimmt ist.<sup>108</sup>
- 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 von einem Cloud-Anbieter übergebener Daten

Grundsätzlich ist festzuhalten, dass die Bekanntgabe von Daten gemäss Artikel 9 DSGVO an den Cloud-Anbieter rechtlich erlaubt ist. Sowohl Artikel 9 DSGVO als auch Artikel 12 DigiV sehen eine Datenbearbeitung durch Dritte unter gewissen Voraussetzungen ausdrücklich vor. Artikel 9 DSGVO 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.<sup>109</sup> Artikel 320 StGB steht einer Auftragsdatenbearbeitung im Sinne von Artikel 9 DSGVO für Personendaten damit grundsätzlich nicht entgegen.<sup>110</sup> 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<sup>111</sup> grundsätzlich zugänglich sind oder ob sie aufgrund spezifischer Rechtsgrundlagen besonderen Anforderungen an die Vertraulichkeit unterliegen (Schutzbedarfs- und Risikoanalyse, vgl. Teil 1, Ziff. 3.1). Darauf gestützt ist festzulegen, welche angemessenen Schutzmassnahmen, insb. technische und organisatorische Massnahmen des Daten- und Informationsschutzes (Art. 12 Bst. c DigiV), zu treffen sind.

<sup>105</sup> 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.

<sup>106</sup> 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 (BGE 135 IV 198, E.3.3.).

<sup>107</sup> BGE 127 IV 122; BSK StGB-Oberholzer, Art. 320 Rz. 8.

<sup>108</sup> BSK StGB-Oberholzer, Art. 320 Rz. 9.

<sup>109</sup> BÜHLER/RAMPINI, Art. 9 DSGVO, Rz. 1.

<sup>110</sup> GA WIDMER, S. 20; RUDIN, S. 83.

<sup>111</sup> Vgl. insb. Art. 10 Entwurf zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben [SR 172.019 - EMBAG](#) betreffend Open Government Data.

### 2.2.2.2 Kenntnisnahme von den Informationen durch den Cloud-Anbieter oder Dritte («Offenbarung»)

Der Zugriff des Cloud-Anbieters auf dem Amtsgeheimnis unterstehende Daten muss im Rahmen eines Cloud-Outsourcing durch vertragliche, organisatorische und technische Massnahmen angemessen beschränkt bzw. soweit möglich minimiert 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 Cloud-Anbieter 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<sup>112</sup>). 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.<sup>113</sup>

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

### 2.2.2.3 Entbindung vom Amtsgeheimnis

Nach Artikel 320 Ziffer 2 StGB ist der Täter nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde offenbart hat. Die Entbindung vom Amtsgeheimnis muss dabei die betreffenden Informationen oder den betreffenden Kontext klar spezifizieren und gilt nur für die davon erfassten Informationen bzw. Daten und gegenüber allenfalls spezifizierten Adressaten. Eine solche Entbindung erfolgt in der Praxis z.B. regelmässig im Rahmen von behördlichen Untersuchungen damit, Zeugen und Auskunftspersonen gegenüber Untersuchungsorganen aussagen dürfen.

### 2.2.2.4 Hilfspersonenstatus des Cloud-Anbieters

Bei der vertraglichen Regelung zwischen Bundesverwaltung und dem Cloud-Anbieter handelt es sich um ein Auftragsverhältnis im privatrechtlichen Sinn. Der Cloud-Anbieter gilt aufgrund der oben dargelegten Rechtsgrundlagen für Outsourcing-Lösungen nicht als unberechtigter Dritter im Sinne von Artikel 320 StGB, sondern ist als Hilfsperson zu qualifizieren.<sup>114</sup>

## 2.3 Schlussfolgerung

Gemäss den vorgehenden Ausführungen stellt die Auslagerung der Daten in die Cloud keine Verletzung des Amtsgeheimnisses nach Artikel 320 StGB dar, sofern die Vorgaben von Artikel 12 DigiV beachtet werden. Mitarbeitende der Bundesverwaltung machen sich demnach bei der Auslagerung von Daten in die Cloud grundsätzlich nicht wegen Amtsgeheimnisverletzung strafbar<sup>115</sup>.

Eine Verletzung des Amtsgeheimnisses ist insbesondere dann möglich, wenn der Cloud-Anbieter seinerseits die Daten unberechtigterweise einem Dritten zugänglich macht oder ihm die Kenntnisnahme ermöglicht.<sup>116</sup> Um dies zu verhindern, gibt es verschiedene Möglichkeiten. Daten können insb. verschlüsselt oder pseudonymisiert (vgl. Teil 2, Ziff. 1.2.2) oder tokenisiert werden. Der Cloud-Anbieter müsste daher in der Regel technische Massnahmen umgehen und würde seine vertraglichen Verpflichtungen verletzen (und möglicherweise auch weitere strafrechtliche Bestimmungen, zu nennen wären etwa Art. 143 [Unbefugte Datenbeschaffung], Art. 271 StGB [Verbotene Handlungen für einen

<sup>112</sup> Z.B. wenn der Auftraggeber diesen Zugriff im Einzelfall genehmigt hat.

<sup>113</sup> SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 28.

<sup>114</sup> Siehe dazu [Botschaft ISG, BBl 2017 2953](#), 3077.

<sup>115</sup> Vgl. dazu auch ZYSSET, S. 17, m.w.H.

<sup>116</sup> Strafbar machen sich in diesem Szenario die verantwortlichen Hilfspersonen beim Anbieter, die seit 1.1.2023 von Art. 320 StGB erfasst werden; vgl. ZYSSET, S. 16.

fremden Staat]<sup>117</sup> oder Art. 272-274 StGB [politischer, wirtschaftlicher oder militärischer Nachrichtendienst]).

Da es sich bei den Cloud-Anbieter hauptsächlich um Unternehmen mit Sitz in Ausland handelt, stellt sich 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.

## 3 Bestimmungen zur Informationssicherheit des Bundes

Das Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG, SR 128) soll Informationen und Informatikmittel des Bundes schützen. Das ISG hat einen weiten institutionellen Geltungsbereich: Es 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 (insb. Departemente, Bundeskanzlei, zentrale und dezentrale Verwaltungseinheiten, samt Armee; 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 in Bezug auf ihre Verwaltungsaufgaben dem ISG unterstellt. Der Bundesrat hat 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 ausgenommen, soweit sie nicht klassifizierte Informationen des Bundes bearbeiten, auf Informatikmittel des Bundes zugreifen oder solche betreiben lassen (Art. 2 Abs. 2 der Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee [Informationssicherheitsverordnung ISV], gestützt auf 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. Art. 9 ISG) bzw. gegebenenfalls dem Betriebssicherheitsverfahren zu unterziehen (Art. 49 ff. ISG).

### 3.1 Allgemeine Bemerkungen

Nach Art. 6 Abs. 2 ISG muss die sichere Bearbeitung aller Informationen und Informatikmittel, für die der Bund zuständig ist (auch die nicht-klassifizierte Informationen), gewährleistet sein. Die zuständigen Stellen sorgen dafür, dass die Informationen ihrem Schutzbedarf entsprechend: nur Berechtigten zugänglich sind (Vertraulichkeit); verfügbar sind, wenn sie benötigt werden (Verfügbarkeit); nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität); nachvollziehbar bearbeitet werden (Nachvollziehbarkeit). 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. Beim Einsatz von Cloud-Providern sollten auch zentrale Aspekte der Informationssicherheit in den Verträgen geregelt werden, gleich wie beim Datenschutz.

Die Massnahmen zur Sicherheit der Informatikmittel sollen jedoch stets zweckmässig und wirtschaftlich sinnvoll sein. Es ist eine Kosten- Nutzenabwägung vorzunehmen.<sup>118</sup>

### 3.2 Sicherheitsverfahren (Art. 16-19 ISG)

Um die Informationssicherheit beim Einsatz von Informatikmitteln zu gewährleisten, insbesondere beim Bezug von Informatikdienstleistungen bei externen Leistungserbringern, sind die Bestimmungen zur «Sicherheit beim Einsatz von Informatikmitteln» nach Artikel 16-19 ISG massgebend. Dabei ist es

<sup>117</sup> Vgl. dazu auch SUVA, S. 8.

<sup>118</sup> Siehe dazu [Botschaft ISG, BBl 2017 2953](#), 3012.

die Aufgabe der verpflichteten Behörden die Anforderungen des Sicherheitsverfahrens näher zu umschreiben (Art. 16 ISG).

Gemäss Artikel 16 ISG legen die verpflichteten Behörden ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln fest, welches insbesondere die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von Informatikmitteln; die Umsetzung von Sicherheitsmassnahmen und deren Überprüfung; die Zuständigkeit für die Sicherheitsfreigabe von Informatikmitteln und das Vorgehen bei Veränderung der Risiken umfasst. Zuständig für die Durchführung des Sicherheitsverfahrens ist diejenige verpflichtete Behörde oder Organisation, wie den Einsatz des Informatikmittels beschliesst, also der Leistungsbezüger (Art. 16 Abs. 3 ISG). Der Leistungsbezüger ist für die Geschäftsprozesse verantwortlich und muss die Geschäfts- und Sicherheitsanforderungen seinem Leistungserbringer klar kommunizieren.

Gemäss Artikel 17 ISG werden die Informatikmittel in drei Sicherheitsstufen unterteilt. Diese Einstufung dient der Identifizierung der Kritikalität eines Informatikmittels in Bezug auf die öffentlichen Interessen gemäss Artikel 1 Absatz 2 ISG. Die Kritikalität wird von der Schwere des Schadens abgeleitet, wenn die Information oder das Informationsmittel missbraucht oder gestört werden (siehe auch Art. 28 ISV). Die Sicherheitsstufe «Grundschatz» gilt für sämtliche Informatikmittel, sofern sie nicht höher eingestuft sind (Art. 17 Abs. 1 ISG). Die Sicherheitsstufe «hoher Schutz» gilt für Informatikmittel, wenn eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen kann oder ein Missbrauch oder eine Störung des Informatikmittels die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen kann. VERTRAULICH klassifizierte Informationen gehören in diese Stufe. (Art. 13 Abs. 2 ISG). Die Sicherheitsstufe «sehr hoher Schutz» gilt für Informatikmittel, wenn eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann oder ein Missbrauch oder eine Störung des Informatikmittels die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann. GEHEIM klassifizierte Informationen gehören in diese Stufe. (Art. 13 Abs. 3 ISG).

Artikel 18 ISG und Artikel 29 ISV regeln die Sicherheitsmassnahmen, welche die verpflichteten Behörden festlegen müssen. Hierbei handelt es sich um ein minimales Sicherheitsniveau, die für sämtliche Informatikmittel gelten sollen. Im Rahmen des Sicherheitsverfahrens muss für den Grundschatz keine detaillierten Risikobeurteilungen durchgeführt werden. Für die Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» ist eine objektbezogene Risikoanalyse jedoch vorausgesetzt. Gestützt auf diese Risikoanalyse ist ein Informationssicherheitskonzept zu erstellen. Die Verantwortung zur Erstellung dieser Dokumente liegt beim Leistungsbezüger in enger Zusammenarbeit mit dem Leistungserbringer, da er die Verantwortung der Umsetzung der technischen Massnahmen trägt. Das Informationssicherheitskonzept muss laufend angepasst werden, um den aktuellen Stand der Sicherheit zu beschreiben. Die Wirksamkeitsprüfung (Absatz 3) ist eine Massnahme mit welcher die Informatiksicherheit getestet werden kann. Das Informatikmittel wird detailliert auditiert.<sup>119</sup> Da eine Auditierung einen erheblichen finanziellen Aufwand generiert, muss sie nur bei kritischen Informatikmitteln<sup>120</sup> durchgeführt werden.

Die Hauptverantwortung für die Sicherheit der Informatikmittel liegt gemäss Artikel 16 Absatz 3 ISG beim Leistungsbezüger. Die Leistungserbringer müssen dafür sorgen, dass im Betrieb die Sicherheit der Informatikmittel nach dem aktuellen Stand der Wissenschaft und der Technik gewährleistet wird. Da die internen Leistungserbringer alle unter dieses Gesetz fallen, müssen sie diese Anforderungen einhalten. Externe Leistungserbringer (wie z.B. Cloudanbieter) gelten als Dritte nach Artikel 9 ISG und müssen vertraglich verpflichtet werden, die Massnahmen des ISG einzuhalten. Bei Verdacht auf Gefährdung oder bei konkreter Verletzung der Informationssicherheit kann es vorkommen, dass Aktivitäten von internen oder externen Mitarbeitern detailliert geprüft werden müssen. Gemäss Artikel 19 Absatz 2 ISG sind Vorschriften des RVOG sinngemäss anwendbar (Art. 57i-57q RVOG).

### 3.3 Auswirkungen für Cloud-Projekte

Das ISG regelt insb. 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

<sup>119</sup> Siehe dazu [Botschaft ISG, BBl 2017 2953](#), 3026 f.

<sup>120</sup> Unter kritischen Infrastrukturen werden Dienstleistungs- und Versorgungssysteme verstanden, die essenziell für die Wirtschaft bzw. die Lebensgrundlagen der Bevölkerung sind (Stromversorgung, medizinische Versorgung, Telekommunikation usw.). Dabei zählen nicht nur Bauten und Anlagen dazu, sondern sämtliche Elemente, die für die Verfügbarkeit der Güter und Dienstleistungen notwendig sind (IT-Systeme, Netzwerke etc.). Kritische Informatikmittel sind ein Teil der kritischen Infrastrukturen. Weitere Informationen finden sich hier: [Die kritischen Infrastrukturen](#).

Informatikmitteln der Sicherheitsstufe «Grundschutz», «hoher Schutz» oder «sehr hoher Schutz» gemäss Artikel 17 ISG zuzuordnen ist<sup>121</sup>.

Insbesondere werden folgende Punkte zu prüfen sein:

*Klassifizierung:* Die Klassifizierungskriterien sind in der Informationssicherheitsverordnung im Detail festgelegt (Art. 16 ff. ISV). Wenn klassifizierte Informationen in der Cloud bearbeitet werden, müssen zusätzliche technische Sicherheitsmassnahmen umgesetzt werden. GEHEIM klassifizierte Daten dürfen nur in der Secure Private Cloud Bund (Stufe IV) bearbeitet werden<sup>122</sup>.

Die *Informatikmittel* (vgl. Art. 5 Bst. a ISG) müssen innerhalb von zwei Jahren nach Inkraftsetzung des ISG nach den neuen Bestimmungen des ISG, also bis Ende 2025, neu eingestuft werden (Art. 90 Abs. 2 Satz 1 ISG; vgl. Art. 16-19 ISG i.V.m. den Bestimmungen der ISV). Technische Massnahmen zur Gewährleistung der Informationssicherheit müssen hingegen erst innerhalb von sechs Jahren nach Inkraftsetzung des ISG umgesetzt werden (vgl. Art. 90 Abs. 2 Satz 2 ISG). Als Informatikmittel gilt auch eine Cloud-Anwendung, womit das ISG und alle entsprechenden Ausführungsbestimmungen auch für Cloud-Projekte zur Anwendung gelangen (siehe oben Teil 2, Ziff. 3.2).

### **3.4 Personensicherheitsprüfung (PSP) und Betriebssicherheitsverfahren (BSV)**

Nebst technischen Sicherheitsanforderungen zählen auch die Personensicherheitsprüfungen (PSP) und das Betriebssicherheitsverfahren (BSV) zu den Sicherheitsmassnahmen. PSP sind bei internen wie auch Dritten vorausgesetzt, sobald die Personen sicherheitsempfindliche Tätigkeiten i.S.v. Artikel 5 Bst. b ISG durchführen. Das BSV wird bei Betrieben, welche für den Bund einen sicherheitsempfindlichen Auftrag (analog Art. 5b ISG) ausführen, durch die Fachstelle Betriebssicherheit (SEPOS) durchgeführt, wobei die auftragnehmenden Betriebe je nach Auftrag und Schutzbedarf der Informationen oder Informatikmittel entsprechende Sicherheitsanforderungen umsetzen müssen. Sicherheitsempfindliche Tätigkeiten sind die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen; die Verwaltung, der Betrieb, die Wartung und die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» (nicht dazu gehört die Benutzung); der Zugang zu Sicherheitszonen nach Artikel 23 ISG, insbesondere zu Schutzzone 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen (Art. 5 Bst. b ISG).

*Personensicherheitsprüfungen (PSP):* Bundesinterne oder Externe Personen, welche sicherheitsempfindliche Tätigkeiten ausführen, benötigen eine PSP. Je nach Tätigkeit und Sicherheitsempfindlichkeit wird eine Grundsicherheitsprüfung oder erweiterte PSP durchgeführt. (vgl. Art. 10 Verordnung über die Personensicherheitsprüfungen, RS 128.31).

Für die Sicherstellung der PSP vom Mitarbeitenden der Bundesverwaltung sind grundsätzlich die im Amt vorgesehenen Rollen, sog. einleitende Stellen, zuständig. Die Fachstelle PSP VBS und BK führen die PSP durch und geben in Form einer Erklärung ihre Bewertung über ein potenziell bestehendes Risiko ab. Die im Amt bezeichnete Stellen (mit Personalverantwortlichkeit), sog. entscheidende Stellen, entscheiden aufgrund der Bewertung der jeweiligen Fachstelle PSP, ob sie das ausgewiesene Risiko übernehmen will oder nicht und trifft die notwendigen Vorkehrungen.

Für die Einleitung und den Entscheid der PSP bei Firmenmitarbeitenden, welche den Auftrag ausführen, sind im Rahmen des BSV die Fachstelle Betriebssicherheit zuständig. Wird auf das BSV aufgrund vereinfachten Sicherheitsanforderungen verzichtet, so sorgt die Projektleitung der auftraggebenden Stelle für die PSP, sofern die Person nicht bereits eine gültige PSP besitzt.

*Betriebssicherheitsverfahren (BSV):* Sobald der Bund das Bedürfnis hat, einen sicherheitsempfindlichen Auftrag Extern zu vergeben, ist ein Antrag auf Einleitung an die Fachstelle Betriebssicherheit zu stellen (Art. 52 ISG). Diese prüft noch vor der Ausschreibung, ob für diesen Auftrag ein umfangreiches BSV, also die Prüfung des Betriebs, durchgeführt werden soll oder nicht. Sobald der Betrieb im Rahmen des BSV die vorausgesetzten Anforderungen umgesetzt hat, erhält er von der Fachstelle Betriebssicherheit eine Betriebssicherheitserklärung in Form einer Verfügung, womit er zur Ausführung des sicherheitsempfindlichen Auftrages berechtigt wird. Dieses Verfahren wurde mit dem Inkrafttreten des ISG vom ehemaligen Geheimschutzverfahren beim VBS auf sämtliche Behörden des Bundes ausgeweitet.

Beide Verfahren sind sehr aufwändig und nehmen unter Umständen viel Zeit in Anspruch.

<sup>121</sup> Vgl. auch AR010, Ziff. 4.2.2, SEC-1 (Sicherheitsverfahren durchführen).

<sup>122</sup> AR010, Ziff. 4.2.2, SEC-2.

Nach bisherigem Recht ausgestellte Betriebssicherheitsklärungen (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 Verordnung über das Betriebssicherheitsverfahren [VBSV; SR 128.41]). Wenn noch gar keine BSE ausgestellt wurde, ist eine solche durchzuführen oder zu prüfen, ob eine solche durchgeführt werden muss (vgl. Verfahren nach der VBSV).

## 3.5 Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen

Das Parlament hat am 29. September 2023 eine Änderung des ISG verabschiedet, die eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen einführt. Die Ausführungsbestimmungen konkretisiert der Bundesrat in der Cybersicherheitsverordnung (CSV), welche derzeit noch erarbeitet wird. Die noch nicht in Kraft gesetzten Änderung des ISG sieht in Artikel 74a ff. ISG vor, dass gewisse Behörden und Organisationen Cyberangriffe melden müssen. Darunter fallen neben den Bundesbehörden (Art. 74b Abs. 1 Bst. b ISG) auch Anbieterinnen und Betreiberinnen von Cloudcomputing, Suchmaschinen, digitalen Sicherheits- und Vertrauensdiensten sowie Rechenzentren, sofern sie einen Sitz in der Schweiz haben (Bst. t) und Herstellerinnen von Hard- oder Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der folgenden Zwecken eingesetzt wird: 1. Steuerung und Überwachung von betriebstechnischen Systemen und Prozessen, 2. Gewährleistung der öffentlichen Sicherheit (Bst. u).

Die Frist zur Meldung eines Cyberangriffes beträgt 24 Stunden nach Entdeckung des Cyberangriffes. Die Meldung kann später mit weiteren Informationen ergänzt werden.<sup>123</sup> Gemeldet werden müssen unter anderem Datum, Uhrzeit, Art des Angriffs, sowie die Auswirkungen des Angriffs und Informationen darüber, ob der Angriff mit Erpressung, Drohung oder Nötigung verbunden war (Art. 74e ISG i.V.m. Art. 19 ISV). Übermittelt werden die Meldungen über ein Kommunikationssystem des BACS. Werden die Meldepflichten verletzt kann dies mit einer Busse bis zu CHF 100'000 bestraft werden (Art. 74h ISG).

### 3.5.1 Auswirkungen für Cloud Projekte

Die Meldepflicht wird unter Umständen auch die Cloudanbieterinnen betreffen, wenn sie einen Sitz in der Schweiz haben oder die Voraussetzungen von Artikel 74b Absatz 1 Buchstabe u ISG erfüllen. Die Implementierung zur Erfüllung dieser gesetzlichen Vorgabe ist Sache der Cloudanbieterinnen. Für die Bundesbehörden ist es jedoch wichtig, dass sie zeitnah von einem, sie betreffenden Vorfall informiert werden, denn auch sie unterstehen der Meldepflicht (Art. 74b Abs. 1 Bst. b ISG). Die Frist der 24 Stunden beginnt ab Kenntnisnahme des Vorfalls zu laufen. Für die Bundesbehörden gilt diese Pflicht, ab der Meldung der Cloudanbieterin an die Bundesbehörden. Damit die Meldung ans BACS nicht doppelt erfolgt (einmal durch die Bundesbehörde und einmal durch die Cloudanbieterin) könnte man sich überlegen die Meldepflichten vertraglich der Cloudanbieterin zu übertragen. Die Verantwortlichkeit für die Einhaltung der Meldepflicht würde jedoch weiter bei der Bundesbehörde liegen.

## 4 Weitere relevante Rechtsgrundlagen

### 4.1 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) und hat in Bezug auf die Bundesverwaltung denselben Geltungsbereich wie das ISG. Die IAMV stützt sich dabei primär auf Artikel 26 und 84 Absatz 1 ISG. Sie regelt in Artikel 5 die Verantwortlichen für die IAM-Systeme in den verschiedenen Bereichen.

<sup>123</sup> Siehe die [Referendumsvorlage BBl 2023 2296](#) sowie [Botschaft zur Änderung des Informationssicherheitsgesetzes, BBl 2023 84, S. 32 ff.](#) Die Referendumsfrist ist am 18.1.2024 unbenutzt abgelaufen, der Bundesrat hat die [Änderung auf den 1. April 2025 in Kraft gesetzt](#).

Der Bereich DTI der BK ist unter anderem verantwortlich für das IAM-System der Supportprozesse Finanzen, Beschaffung, Immobilien und Logistik einschliesslich der Cloud-Anbindungen (Art. 5 Abs. 1 Bst. a Ziff. 2 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 einem 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.<sup>124</sup> Artikel 18 IAMV regelt noch die Anforderungen an die Informationssicherheit. Die IAMV regelt somit bereits explizit den Fall der Auslagerung von Daten und in die Cloud und erlaubt diese für IAM-Systeme unter Einhaltung der in Artikel 17ff. IAMV genannten Voraussetzungen.

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

Die Artikel 57i ff. Regierungs- und Verwaltungsorganisationsgesetz (RVOG, SR 172.010) regeln die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen (sog. Randdaten) subsidiär, soweit kein anderes Bundesgesetz eine Regelung trifft. Artikel 57j Absatz 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 57i – 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. Artikel 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 (VBNIB, SR 172.101.442) 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.

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.

<sup>124</sup> Dazu gehört unter anderem die vorgängige Information der betroffenen Personen (Art. 17 Abs. 4 IAMV).

### 4.3 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).

### 4.4 Weisungen mit Geltung für die gesamte Bundesverwaltung

Die Cloud-Prinzipien der Bundesverwaltung (AR010) enthalten neben Empfehlungen und Hinweisen verschiedene Vorgaben mit Weisungscharakter:

- Sourcing und Beschaffung von IaaS und PaaS-Diensten muss zwingend über von DTI bewilligte Cloud Service Broker (CSB) erfolgen (Ziff. 4.1.1 und 4.1.2)
- Definition einer Exit-Strategie: Die zuständige Verwaltungseinheit muss mit Unterstützung des verantwortlichen CSB eine Exit-Strategie definieren (Ziff. 4.1.3)

Als weitere wichtige Vorgabe ist der IT-Grundsatz der Bundesverwaltung<sup>125</sup> zu nennen, der für alle Verwaltungseinheiten verbindlich einzuhalten ist und sich auf Artikel 16 Absatz 2 ISG stützt (vgl. Teil 2, Ziff. 3).

Verschiedene weitere 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 40 Absatz 1 DigiV stützen. Davon sind insbesondere die E027 – Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)<sup>126</sup> oder die E026 – Einsatzrichtlinie Arbeitsplatzsystem von möglicher Bedeutung.<sup>127</sup> Diese Einsatzrichtlinien konkretisieren jedoch übergeordnetes Recht und es ergeben sich daraus keine neuen Rechte und Pflichten für die Verwaltungseinheiten.

<sup>125</sup> Siehe [Si001-IT-Grundsatz\\_V5-0-d\(4\).pdf](#).

<sup>126</sup> Siehe [Einsatzrichtlinie E027 1-1 \(1\).pdf](#).

<sup>127</sup> Siehe [E026 1-1 GENEHMIGT d \(1\).pdf](#).

## Anhang A Literatur und Materialien

AMT FÜR INFORMATIK UND ORGANISATION (KAIO)	Restrisiken beim Einsatz von M365 <a href="#">Bericht an den Regierungsrat.</a>
BAERISWYL BRUNO	Art. 9 DSG, in: Datenschutzgesetz (DSG) (ders./PÄRLI/BLONSKI, Hrsg.), 2.A. 2023.
BRAUNECK JENS	Europa-Cloud: Zwingt der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe?, in: Europäisches Wirtschafts- und Steuerrecht, 2019.
BÜHLER ROBERT/RAMPINI CORRADO	Art. 9 DSG, in: BLECHTA/VASELLA (Hrsg.), Basler Kommentar DSG und BGÖ, 4. A., 2024.
BUNDESAMT FÜR JUSTIZ (BJ)	<a href="#">Bericht zum US CLOUD Act</a> , Gutachten des Bundesamtes für Justiz vom 17. September 2021.
BUNDESAMT FÜR JUSTIZ (BJ)	Bericht zur e-Evidence-Vorlage der EU, 24. Oktober 2023.
BUNDESAMT FÜR JUSTIZ UND EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (BJ/EDÖB)	<a href="#">Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen.</a>
BUNDESKANZLEI (DIGITALE TRANSFORMATION UND IKT-LENKUNG DTI)	AR010 – Cloud-Prinzipien der Bundesverwaltung (V1.1 vom 13.3.2025; zit. AR010).
BUNDESRAT	Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, <a href="#">BBI 2017 6941</a> (Botschaft Totalrevision DSG).
BUNDESRAT	Botschaft zum Bundesgesetz über die Informationssicherheit, BBI 2017 2953 (Botschaft ISG).
BURRI MIRA	Creating Data Flow Rules through Preferential Trade Agreements, in: Data Sovereignty (CHANDER/SUN, Hrsg.), 2023, S. 264 ff.
CHANDER ANUPAM/SUN HAOCHE	Introduction: Sovereignty 2.0, in: Data Sovereignty (CHANDER/SUN, Hrsg.), 2023, S. 1 ff.
CHEN BING/LIU YONGJI	Promotion and Advancement of Data Security Governance in China, in: Electronics 2024, 13, 1905, verfügbar unter <a href="https://doi.org/10.3390/electronics13101905">https://doi.org/10.3390/electronics13101905</a> (14.3.2025).
DICKINSON STEVE	China's new cybersecurity law: no place to hide, 11. Oktober 2020, verfügbar unter <a href="https://harrisbricken.com/chinalawblog/china-cyber-security-no-place-to-hide/">https://harrisbricken.com/chinalawblog/china-cyber-security-no-place-to-hide/</a> (14.3.2025).
HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX	Allgemeines Verwaltungsrecht, 8. Auflage, Zürich/St. Gallen, 2020.
HILLMANN JONATHAN E.	Digital Silk Road, London, 2021.
JAAG TOBIAS	Bedarfsverwaltung, in: Kommunikation. Festschrift für Rolf Weber zum 60. Geburtstag (SETHE et al., Hrsg.), Bern, 2011, S. 543 ff.
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, verfügbar unter Cloud Gutachten LLAG für OIZ (Sep 2021) mit Zusätzen (Nov 2021) (lauxlawyers.ch).

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

DIESELBEN	Aktennotiz zum Gutachten Schefer/Glass; Grundrechtskonformer Einsatz von M365 durch Gemeinden
LI WENLONG/CHEN JIAHONG	From brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China, in: Computer Law & Security Review, Volume 54, 2024, verfügbar unter <a href="https://www.sciencedirect.com/science/article/pii/S026736492400061X">https://www.sciencedirect.com/science/article/pii/S026736492400061X</a> (14.3.2025).
LOBSIGER ADRIAN	Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, in: SJZ 6/2023, S. 311 ff.
MILLARD CHRISTOPHER	Cloud Computing Law, 2. Auflage, Oxford University Press, 2021.
BUNDESAMT FÜR CYBERSICHERHEIT	<a href="#">Si001 IT-Grundschutz in der Bundesverwaltung vom 1.3.2022</a> (V 5.1 vom 5.7.2024), (zit.: BACS, Si001).
BUNDESAMT FÜR CYBERSICHERHEIT	E026 Einsatzrichtlinie Arbeitsplatzsystem (zit.: BACSE026).
NZZ	China baut weltweit ersten «Freihafen für Daten», 21.1.2022.
PERLROTH NICOLE	The Cyber Weapons Arms Race, London, 2021, S. 320 ff.
SCHEFER/GLASS	Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich.
ROSENTHAL DAVID	Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act; in: Jusletter 10. August 2020 (zit.: ROSENTHAL, US CLOUD Act).
DERSELBE	Schweizer Banken in die Cloud, in: Vischer 9. September 2021, verfügbar unter <a href="https://www.vischer.com/know-how/blog/schweizer-banken-in-die-cloud-so-geht-es-und-so-nicht-39214/">https://www.vischer.com/know-how/blog/schweizer-banken-in-die-cloud-so-geht-es-und-so-nicht-39214/</a> (zit.: ROSENTHAL, Schweizer Banken in die Cloud; 14.3.2025).
DERSELBE	Frequently Asked Questions (FAQ) on the Risk of Foreign Lawful Access and the Statistical “Rosenthal” Method for Assessing it, Version 23. Oktober 2022, verfügbar unter <a href="https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf">https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf</a> (zit.: ROSENTHAL, FAQ; 14.3.2025).
DERSELBE	<a href="#">Anmerkungen Rosenthal zum Gutachten Schefer/Glass zu «M365»</a> (14.3.2025).
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.
SUVA	Antwortschreiben zur Stellungnahme EDÖB betr. M365, verfügbar unter <a href="http://www.edoeb.admin.ch">www.edoeb.admin.ch</a> , <a href="#">Auslagerung von Personendaten durch die Suva in eine Microsoft Cloud</a> (14.3.2025).
VON WALTER AXEL	Executive Order, in: Datenschutzberater (DSB), 2022, S. 294 ff.

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

WIDMER URSULA	Gutachten Klärung und Analyse der rechtlichen Grundlagen für die Integration von «Plattform-as-a-Service» und «Software-as-a-Service» in der öffentlichen Verwaltung für die Schweizerische Informatikkonferenz (SIK), 2018.
ZYSSET ESTHER	Der behördliche Gang in die Cloud – Betrachtungen zur Auslegung im öffentlichen Sektor, in: Jusletter 23. September 2024.

## 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. Zu verschiedenen Methoden vgl. Teil 1 Ziff. 2.2
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 Eindämmung bzw. 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 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.