UNIVERSITÄT
BERN

Vorgehen bei der Auslagerung von Datenbearbeitungen – Clouds everywhere?

Eine Bedienungsanleitung für staatliche Institutionen

MAS-Arbeit eingereicht der Universität Bern
im Rahmen des Executive Master of Public Administration (MPA)

Betreuender Dozent: **Prof. Claus D. Jacobs, Ph.D.**
Kompetenzzentrum für Public Management
Schanzeneckstrasse 1
CH-3001 Bern

Verfasserin: **Dr. iur. Dominika Blonski**

Zürich, 29. April 2023

Management Summary

Die MAS-Arbeit betrachtet die Frage, welche Aspekte durch öffentliche Institutionen zu berücksichtigen sind, wenn diese die Nutzung von neuen Technologien – am Beispiel von Cloud-Lösungen – in Erwägung ziehen, aus fünf Perspektiven (staatstheoretisch, politisch, strategisch, juristisch und technisch). Damit lassen sich die Rahmenbedingungen für eine Auslagerung in eine Cloud aufzeigen. Als konzeptionelle Arbeit resultiert sie in einer Handlungsanleitung.

Der Staat hat ich bei seiner Aufgabenerfüllung an die verfassungsmässigen Prinzipien (insbesondere die Grundrechte und das Legalitätsprinzip) zu halten. Denn die Stellung des Staates unterscheidet sich von jener privater Akteure aufgrund des Unter-/Überordnungsverhältnis, der fehlenden Wahlmöglichkeit der Individuen sowie der fehlenden Freiwilligkeit. Damit trägt der Staat eine besondere Verantwortung und muss diese auch im Rahmen der Auslagerung wahrnehmen.

Somit hat der Staat bei Beschaffungen nach einem klar definierten Prozess vorzugehen und die Anforderungen, die sich für ihn bei der Auslagerung – insbesondere auch wenn Cloud-Lösungen beigezogen werden – ergeben, in der Ausschreibung als Muss-Kriterien aufzulisten. Anbieterinnen, die diese Anforderungen nicht erfüllen können, kann der Zuschlag nicht erteilt werden.

Weiter hat er sich strategische Überlegungen zu machen. Bei Cloud-Lösungen können durch Lock-In-Effekte Abhängigkeiten von der Anbieterin sowie Kontroll- und Transparenzverlust entstehen. Zudem ist die Datensouveränität in Frage gestellt.

Cloud Computing ist eine Auftragsdatenbearbeitung. Sie bringt grössere Risiken mit sich, als andere Auslagerungen. Dennoch verbleibt die Verantwortung beim Auftraggeber Staat. Die Gesetze sehen aus diesem Grund klare Voraussetzungen für die grundsätzlich zulässige Auftragsdatenbearbeitung vor. Es sind zwei Bedingungen, die erfüllt sein müssen, damit in die Cloud ausgelagert werden kann. Es dürfen keine rechtlichen Bestimmungen entgegenstehen und die Verantwortung des Auftraggebers muss wahrgenommen werden. Beim ersten Punkt stehen Geheimnispflichten (Amtsgeheimnis, besondere Amtsgeheimnis, Berufsgeheimnis) wie auch vertragliche Vereinbarungen, eine Klassifizierung von Informationen oder weitere Regelungen im Vordergrund. Steht eine rechtliche Bestimmung entgegen, kann geprüft werden, ob eine technische Massnahme die Kenntnisnahme verhindern kann (Verschlüsselung mit Schlüsselmanagement bei der öffentlichen Institution, Anonymisierung oder Pseudonymisierung) und falls ja dennoch ausgelagert werden kann. Die zweite Bedingung erfordert, dass die staatliche Institution bei der Auswahl der Auftragsnehmerin ihre Sorgfaltspflicht wahrnimmt, vertraglich mit ihr die vorgegebenen Themen vereinbart und sich vergewissert, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann.

Bei der Auslagerung in die Cloud ist methodisch sauber vorzugehen. Es sind eine Rechtsgrundlagenanalyse, eine Schutzbedarfs- und Risikoanalyse, ein ISDS-Konzept sowie eine Datenschutz-Folgenabschätzung zu erstellen bzw. durchzuführen. Ergibt diese, das besondere Risiken für die betroffenen Personen vorliegen, ist das Projekt der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

Beim Einsatz von Cloud-Lösungen spielt – wenn die Anbieterin eine US-amerikanische Unternehmung ist – zudem der CLOUD Act eine Rolle. Diese amerikanische Gesetzgebung verstösst gegen den ordre public der Schweiz. In diesen Fällen ist die Kenntnisnahme mittels technischer Lösungen (Verschlüsselung mit Schlüsselmanagement beim Auftraggeber, Anonymisierung oder Pseudonymisierung) bei Anwendbarkeit des Berufsgeheimnisses sowie von besonderen Amtsgeheimnissen auszuschliessen. Bei Vorliegen des Amtsgeheimnisses müssen angemessene organisatorisch-technische Massnahmen ergriffen werden. Der Problematik des CLOUD Acts kann nicht mit Wahrscheinlichkeitsberechnungen begegnet werden. Damit wird verkannt, dass ein öffentliches Organ das Recht immer zu beachten und sich rechtmässig zu verhalten hat (Legalitätsprinzip), und andererseits kann das Verhalten einer amerikanischen Strafbehörde mit einer Methode mit Wahrscheinlichkeitsberechnungen nicht vorausgesagt werden. Nicht eingehaltenes Recht kann nicht durch tiefe Wahrscheinlichkeiten geheilt werden.

Inhaltsverzeichnis

Management Summary II
Inhaltsverzeichnis IV
Abbildungsverzeichnis VI
Tabellenverzeichnis VII
Abkürzungsverzeichnis VIII
1. Einleitung 1
1.1. Ausgangslage, Problemstellung und Fragestellung 1
1.2. Forschungsfrage, Zielsetzung der Arbeit und Abgrenzung 2
1.3. Methodisches Vorgehen 2
1.4. Aufbau der Arbeit 3
2. Cloud Computing 4
2.1. Definition von Cloud Computing 4
2.2. Aus technischer Perspektive 5
2.2.1. Merkmale von Cloud Computing 5
2.2.2. Servicemodelle von Cloud Computing 5
2.2.3. Arten von Cloud Computing 7
2.3. Aus juristischer Perspektive 8
3. Auslagerung beim Staat 9
3.1. Was den Staat zum Staat macht 9
3.1.1. Einteilung des Rechtsstoffs 9
3.1.2. Definition des Staates 10
3.1.3. Stellung des Staates 10
3.1.4. Verfassungsmässige Prinzipien 10
3.1.5. Unterscheidung zu privaten Akteuren 12
3.2. Staatliche Aufgabenerfüllung 12
3.2.1. Definition von staatlichen Aufgaben 12
3.2.2. Arten von staatlichen Aufgaben 13
3.2.3. Arten der staatlichen Aufgabenerfüllung 13

3.3. Auslagerung von staatlichen Aufgaben 14
3.4. Beschaffungswesen 14
3.4.1. Rechtsgrundlagen 15
3.4.2. Vorgehen 15
3.4.3. Beschaffung von IT-Dienstleistungen 16
3.5. Strategische Überlegungen bei der Auslagerung 17
3.6. Politische Überlegungen bei der Auslagerung 19
4. Auftragsdatenbearbeitung 21
4.1. Arten der Auftragsdatenbearbeitung 22
4.2. Cloud Computing als Auftragsdatenbearbeitung 23
4.3. Anwendbares Datenschutzrecht 23
4.4. Rechtliche Grundlagen für die Auftragsdatenbearbeitung 24
4.5. Voraussetzungen für die Auftragsdatenbearbeitung 25
4.5.1. Keine entgegenstehende rechtliche oder vertragliche Bestimmung 25
4.5.2. Wahrnehmung der Verantwortung 28
4.6. Methodisches Vorgehen 31
4.7. Auslagerungen mit Auslandbezug 32
4.7.1. Auslagerung ins Ausland 33
4.7.2. Auslagerung bei Anwendbarkeit des CLOUD Act 33
5. Handlungsanleitung 36
6. Vorgehensweise am Beispiel eines Spitals 38
7. Schlussfolgerungen und Zusammenfassung 41
Literaturverzeichnis IX
Rechtsquellenverzeichnis XI
Selbstständigkeitserklärung XIII
Über die Autorin XIV

Abbildungsverzeichnis

Abbildung 1: Cloud Computing Servicemodelle 6
Abbildung 2: Cloud Computing Organisationsmodelle 7
Abbildung 3: Beschaffungszyklus 16
Abbildung 4: Strategiedreieck 18

Tabellenverzeichnis

Tabelle 1: Handlungsanleitung..... 36
Tabelle 2: Anwendung Handlungsanleitung auf Spital..... 38

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
Aufl.	Auflage
bzw.	beziehungsweise
d.h.	das heisst
Dr. iur.	Doctor iuris
DSFA	Datenschutz-Folgenabschätzung
f./ff.	und folgende (Seite(n), Randnote(n))
Hrsg.	Herausgeber/innen
IaaS	Infrastructure as a Service
ISDS-Konzept	Informationssicherheits- und Datenschutz-Konzept
i.S.v.	im Sinne von
IT	Information Technology
i.V.m.	in Verbindung mit
lit.	littera
LS	Loseblattsammlung (Zürcher Gesetzesammlung)
MAS	Master of Advanced Studies
MPA	Executive Master of Public Administration
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
Prof.	Professor
Ph.D.	Philosophiae Doctor
RRB	Regierungsratsbeschluss

Rn.	Randnote
S.	Seite
SR	Systematische Sammlung des Bundesrechts
SaaS	Software as a Service
Seco	Staatssekretariat für Wirtschaft
SHK	Stämpflis Handkommentar
US	United States
usw.	und so weiter
V	Version
z.B.	zum Beispiel

1. Einleitung

1.1. Ausgangslage, Problemstellung und Fragestellung

In Zeiten der Digitalisierung nutzen auch öffentliche Institutionen neue Technologien – wie beispielsweise Clouds – und arbeiten entsprechend. Mitarbeitende sollen von überall Zugriff auf die Informationen haben, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Corona-Pandemie hat diese Entwicklung stark geprägt, beschleunigt und weiterentwickelt. Der Staat steht damit mitten in einem sich wandelnden Umfeld. Das staubige Papier-Büro gehört der Vergangenheit an. Die Arbeitsweise von Mitarbeitenden und damit des Staates hat sich rasch und bedeutend verändert – es folgt New Work 4.0. Es wird remote von Zuhause, unterwegs oder eben im Büro, das auch mobil sein kann, gearbeitet.

Da der Staat an andere Vorgaben als private Unternehmen gebunden ist, stellen sich zahlreiche Fragen, wie der Staat sich in diesem sich wandelnden Umfeld positionieren kann und will. Wie unterscheiden sich die Vorgaben für den Staat von jenen für Private? Wie kann der Staat die sich verändernden Anforderungen und Bedürfnisse umsetzen? In welchen Konstellationen kann und soll der Staat Externe beiziehen und eine Tätigkeit auslagern? Welche Technologien können wofür unter welchen Bedingungen eingesetzt werden? Wie ist bei der Management-Entscheidung, bestimmte Technologien einzusetzen, konkret vorzugehen und was ist zu berücksichtigen? Welche Strategien können dabei verfolgt werden? Welche rechtlichen Rahmenbedingungen sind dabei zu berücksichtigen?

Diese Entwicklung der Digitalisierung führt aktuell dazu, dass neben dem Bund auch zahlreiche Kantone und Gemeinden Cloud-Lösungen einsetzen möchten, damit ihre Mitarbeitenden für ihre Aufgabenerfüllung online auf die Informationen zugreifen können. Entsprechende Projekte sind geplant oder bereits in der Umsetzung. Solche Cloud-Lösungen werden meist nicht von den öffentlichen Institutionen selber erstellt, sondern die öffentlichen Institutionen greifen auf sich auf dem Markt befindende Angebote zurück. Mit diesem Beizug einer Cloud-Dienstleisterin findet somit eine Auslagerung statt. Diese Auslagerung umfasst auch die Auslagerung der Datenbearbeitung. Somit stellen sich beim Einsatz von Cloud-Lösungen insbesondere auch datenschutzrechtliche und informationssicherheitstechnische Fragen.

Obwohl bei dieser Auslagerung der Datenbearbeitung klare Vorgaben bestehen, stellen die Projekte für die öffentlichen Institutionen eine grosse Herausforderung dar. Es stellt sich den öffentlichen Institutionen die Frage: Welches ist die beste Vorgehensweise, um alle Aspekte im richtigen Moment und wie vorgeschrieben einzubeziehen?

1.2. Forschungsfrage, Zielsetzung der Arbeit und Abgrenzung

Die vorliegende MAS-Arbeit deckt die Frage ab, ob und unter welchen Bedingungen Cloud-Lösungen im Rahmen einer Auslagerung durch den Staat eingesetzt werden können. Für die Beantwortung dieser Frage werden folgende Perspektiven einbezogen und gestützt darauf ein Entscheidungspfad erarbeitet:

- **Staatstheoretische Perspektive** – Was macht den Staat zum Staat?
- **Politische Perspektive** – Welchen Einfluss hat die Politik auf staatliche Entscheidfindung?
- **Strategische Perspektive** – Wie kann der Staat sicherstellen, dass er seine Aufgaben erfüllen kann?
- **Juristische Perspektive** – Welche Vorgaben macht das Recht und insbesondere das Datenschutzrecht?
- **Technische Perspektive** – Wie kann die Technik unterstützen, damit der Staat die Vorgaben einhalten kann?

Folgende **Forschungsfrage** steht im Zentrum der vorliegenden Arbeit:

> *Welche Aspekte sind durch öffentliche Institutionen zu berücksichtigen, wenn diese die Nutzung von neuen Technologien – am Beispiel von Cloud-Lösungen – in Erwägung ziehen?*

Die MAS-Arbeit soll öffentlichen Institutionen eine Anleitung zur Verfügung stellen, die sie bei der Entscheidung für den Einsatz und die Umsetzung von neuen Technologien am Beispiel von Cloud-Lösungen begleitet. Die Arbeit soll dazu beitragen, dass staatliche Institutionen eine klare, einfache Anleitung zur Hand haben, wenn sie neue Technologien nutzen möchten. Diese Anleitung soll sie durch den Prozess führen und ihnen eine Grundlage bieten, die richtigen sich stellenden Fragen im richtigen Moment zu adressieren und Entscheide zu treffen, um diesen Fragen zu begegnen.

Die Arbeit fokussiert auf die Thematik der Auslagerung. Sie bezieht dazu grundlegende und allgemeine Ausführungen ein. Sie stellt den Sonderfall der Auslagerung von Datenbearbeitungen in den Vordergrund und vertieft diese Thematik am Beispiel des Einsatzes von Cloud-Lösungen. Damit geht die Arbeit – unter der Berücksichtigung der verschiedenen Perspektiven – vom Allgemeinen zum Besonderen vor und lässt andere Themenfelder aus.

1.3. Methodisches Vorgehen

Die Themenfelder werden zunächst theoretisch aufgearbeitet. Damit wird die Grundlage für das Vorgehen und den Entscheidungsprozess gelegt. Jede Perspektive gibt dem Staat Vorgaben und Leitlinien, an denen er sich orientieren muss. Die sich ergebenden Fragestellungen können anhand dieser Vorgaben und Leitlinien beantwortet werden. Die Perspektiven zeigen die Vorgaben vor und leiten staatliche Institutionen bei der Entscheidfindung.

Es handelt sich um eine konzeptionelle Arbeit. Sie soll ein Vorgehenskonzept aufzeigen, das als Leitfaden eingesetzt werden kann.

1.4. Aufbau der Arbeit

Die MAS-Arbeit wird von einer Einleitung und einer Schlussfolgerung umrahmt und gliedert sich im Kern im Wesentlichen in fünf Teile:

- Cloud Computing
- Auslagerung beim Staat
- Auftragsdatenbearbeitung
- Handlungsanleitung
- Vorgehensweise am Beispiel eines Spitals

Zunächst wird das Cloud Computing definiert und sowohl aus technischer wie auch juristischer Perspektive beleuchtet.

Anschliessend werden die Grundlagen für das staatliche Handeln dargelegt und anhand von staatstheoretischen und -rechtlichen Ausführungen die Unterschiede zum privaten Sektor aufgezeigt. In diesem Teil werden auch die allgemeinen Grundlagen für die Auslagerung der Aufgabenerfüllung durch staatliche Institutionen dargelegt. Schliesslich setzt sich dieser Teil mit Fragen des Beschaffungswesens sowie strategischen und politischen Überlegungen bei der Auslagerung auseinander.

Im folgenden Hauptteil der Arbeit findet eine Auseinandersetzung mit den datenschutzrechtlichen und -technischen Anforderungen bei der Auslagerung allgemein sowie beim Beizug von Cloud-Lösungen im Besonderen statt. Dabei wird sowohl aus juristischer als auch aus technischer Perspektive ausgewertet, einerseits welche Vorgaben das Datenschutzrecht macht und andererseits wie diese Vorgaben mit technischen Mitteln unterstützt werden können.

Diese Abhandlungen fliessen schliesslich in eine Handlungsanleitung, die das Vorgehen des Staates bei der Auslagerung von Datenbearbeitungen in die Cloud Schritt für Schritt darstellt. Diese Anleitung soll den Herausforderungen, die sich spezifisch beim Staat ergeben, Rechnung tragen.

Der abschliessende folgende Teil zeigt die Vorgehensweise am Beispiel eines Spitals konkret auf. Die Handlungsanleitung wird dabei aus der Perspektive des Spitals durchgearbeitet und zeigt die konkrete Anwendung praxisbezogen auf.

2. Cloud Computing

Cloud Computing ist in aller Munde. Nicht nur Private sondern auch immer mehr öffentliche Institutionen möchten von den Vorzügen der neuen Technologie profitieren. Doch wie definiert sich Cloud Computing? Welche Arten von Cloud Computing gibt es? Und wozu wird Cloud Computing eingesetzt?

Nach einer Definition von Cloud Computing behandeln die folgenden Kapitel einerseits die technische und andererseits die juristische Perspektive auf Cloud Computing.[1]

2.1. Definition von Cloud Computing

Das amerikanische National Institute of Standards and Technology (NIST), das als Teil des U.S. Department of Commerce für Standardisierungsprozesse zuständig ist, definiert Cloud Computing wie folgt:

> *«Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.»*[2]

Damit liegt Cloud Computing vor, wenn allgegenwärtig, bequem, bedarfsorientiert auf ein Netzwerk zugegriffen werden kann. Dieses Netzwerk stellt dabei einen gemeinsam genutzten Pool konfigurierbarer Computerressourcen (z.B. Netzwerke, Server, Speicher, Anwendungen und Dienste) dar, die mit minimalem Verwaltungsaufwand und minimaler Interaktion schnell bereitgestellt und freigegeben werden können.

Cloud Computing ermöglicht damit insbesondere Flexibilität und Skalierbarkeit. D.h. es kann orts- und zeitunabhängig zugegriffen werden und die Rechenkapazitäten können je nach Bedarf zur Verfügung gestellt werden. Dies ermöglicht beispielsweise, dass Mitarbeitende ausserhalb der Büroräumlichkeiten auf in der Cloud gespeicherte Informationen zugreifen können und so ihrer Arbeit nachgehen können. Dies bewirkt auch, dass Ressourcen nur je nach Bedarf bezogen und bezahlt werden können.

---

[1] Für detailliertere Ausführungen: DOMINIKA BLONSKI, Cloud Computing. Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Künstliche Intelligenz und Datenschutz. L'intelligence artificielle et protection des données, Tagungsband zum Dreizehnten Schweizerischen Datenschutzrechtstag, 2. Oktober 2020, Universität Fribourg, Schulthess 2021, S. 65 ff.

[2] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), The NIST Definition of Cloud Computing, Special Publication 800-145, 2011, S. 2, abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (zuletzt besucht am 29.04.2023).

2.2. Aus technischer Perspektive

2.2.1. Merkmale von Cloud Computing

Aus technischer Sicht handelt es sich um Cloud Computing, wenn eine IT-Dienstleistung folgende Charakteristiken zeigt:[3]

- **On-Demand-Self-Service**: Dienstleistungen wie Serverzeit oder Netzwerkspeicher können automatisch angefordert werden,
- **Broad Network Access**: Dienste sind mittels Standardmechanismen über ein Netzwerk zugänglich mit Zugriffsmöglichkeiten über heterogene Client-Plattformen,
- **Resource Pooling**: mehrere Kunden können durch Bündelung der Computing-Ressourcen mit einem mandantenfähigen Modell bedient werden, wobei der Kunde weder Kontrolle noch Kenntnis über den genauen Standort der bereitgestellten Ressourcen hat,
- **Rapid Elasticity**: Dienste können automatisch, flexibel und schnell freigegeben werden,
- **Measured Service**: Messverfahren steuern und optimieren die Nutzung der Dienste.

2.2.2. Servicemodelle von Cloud Computing

Bis vor einigen Jahren waren sogenannte «On Premises»-Nutzungs- und Lizenzmodelle Standard. Dabei werden serverbasierte Computerprogramme lokal in eigener Verantwortung auf eigener Hardware, gegebenenfalls in einem eigenen Rechenzentrum oder auf gemieteten Servern eines fremden Rechenzentrums betrieben. Die Hardware wird dabei nicht vom Anbieter der Software bereitgestellt.

Beim Cloud Computing werden verschiedene Dienstleistungen nicht mehr in eigener Verantwortung auf eigener Hardware betrieben, sondern bei einer externen Anbieterin. Je nachdem, wie viele und welche der Dienstleistungen von der externen Anbieterin übernommen und betrieben werden, unterscheiden sich die Servicemodelle von Cloud Computing.

Es gibt drei Servicemodelle von Cloud Computing:[4]

- **Infrastructure as a Service (IaaS):**
  - Nutzungszugang zu IT-Dienstleistungen mit Computerhardware-Ressourcen wie Rechnern, Netzen und Speicher
  - Ausführung beliebiger Software in eigene Verantwortung
  - Miete von Infrastruktur je nach Bedarf (on demand, skalierbar)
- **Platform as a Service (PaaS):**
  - Nutzungszugang zu Programmierungs- oder Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten

---

[3] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), The NIST Definition of Cloud Computing, Special Publication 800-145, 2011, S. 2, abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (zuletzt besucht am 29.04.2023).

[4] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), The NIST Definition of Cloud Computing, Special Publication 800-145, 2011, S. 2 f., abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (zuletzt besucht am 29.04.2023).

- Eigenen Software-Anwendungen oder Ausführung in Softwareumgebung, die von der Dienstanbieterin (Service-Provider) bereitgestellt und unterhalten wird
- Aufbauend auf einer skalierbaren Infrastruktur (IaaS) von Speicher und Rechenleistung

- **Software as a Service (SaaS):**
  - Nutzungszugang zu standardisierten Software-Sammlungen und Anwendungsprogrammen
  - Sowohl die Software als auch die IT-Infrastruktur wird von der Anbieterin betrieben

Bildlich lassen sich die Servicemodelle wie folgt darstellen:

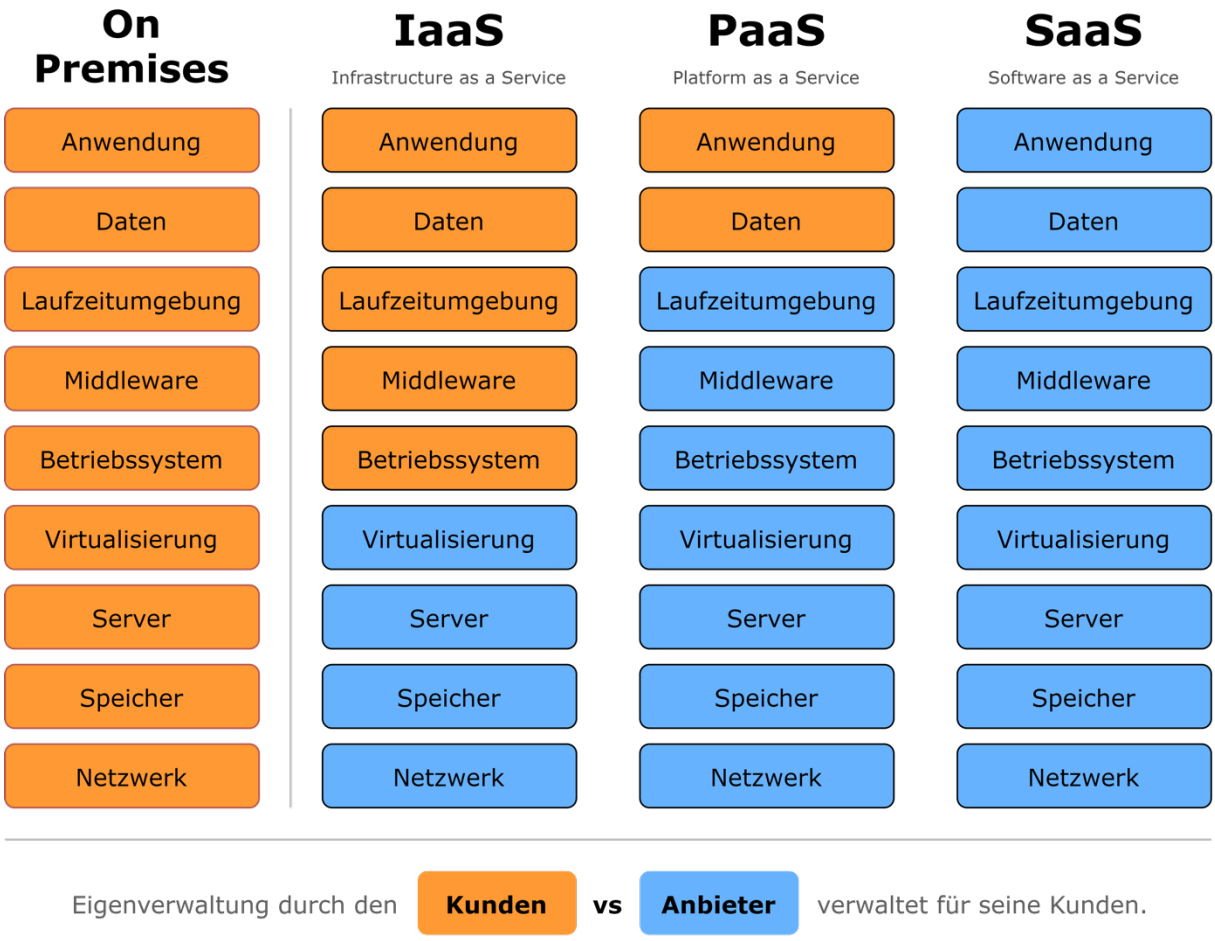

Abbildung 1: Cloud Computing Servicemodelle[5]

[5] Wikimedia Commons, abrufbar unter: <https://commons.wikimedia.org/wiki/File:Cloud_Computing_Servicemodelle.png> (zuletzt besucht am 29.04.2023).

2.2.3. Arten von Cloud Computing

Es können vier Organisationsmodelle von Cloud Computing unterschieden werden:[6]

- **Public Cloud**: Cloud-Infrastruktur wird der breiten Öffentlichkeit über das Internet zur Benutzung bereitgestellt,
- **Private Cloud**: Cloud-Infrastruktur wird exklusiv einer einzelnen Organisation über ein Intranet (Virtual Private Network) zur Verfügung gestellt und damit ausschliesslich für diese eine Organisation betrieben,
- **Community Cloud**: Cloud-Infrastruktur wird exklusiv für eine spezifische Gemeinschaft von Organisationen (z.B. mehrere staatliche Behörden, Universitäten), die gemeinsame Anliegen haben, bereitgestellt,
- **Hybrid Cloud**: besteht aus zwei oder mehreren unterschiedlichen Cloud-Infrastrukturen (Public, Private oder Community), bleiben für sich eigenständig, können aber über standardisierte Schnittstellen gemeinsam genutzt werden.

In Bildern lassen sich die unterschiedlichen Organisationsmodelle wie folgt darstellen:

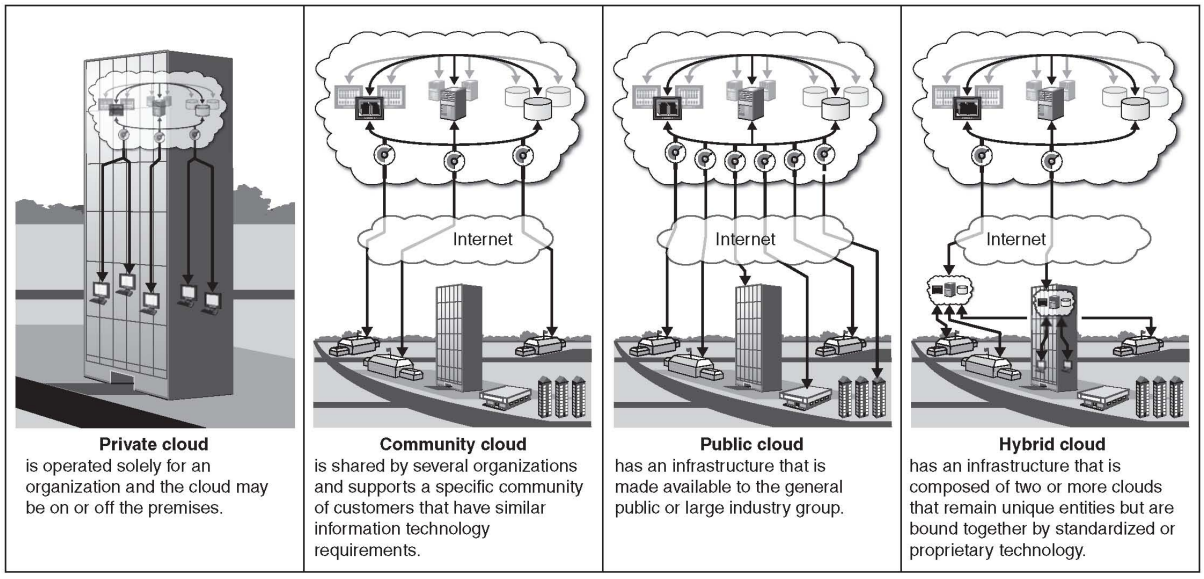

Abbildung 2: Cloud Computing Organisationsmodelle[7]

[6] NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), The NIST Definition of Cloud Computing, Special Publication 800-145, 2011, S. 3, abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (zuletzt besucht am 29.04.2023).

[7] Wikimedia Commons, abrufbar unter: <https://commons.wikimedia.org/wiki/File:Figure_2_Cloud_Computing_Deployment_Models_%286302962481%29.jpg> (zuletzt besucht am 29.04.2023).

2.3. Aus juristischer Perspektive

Aus juristischer Perspektive stellt der Beizug einer Cloud-Dienstleisterin zunächst eine Auslagerung dar. Wie bei jeder Auslagerung wird auch beim Cloud Computing ein Teil der Aufgaben an eine Dritte übertragen. Diese Auftragnehmerin erfüllt diese Aufgaben für den Auftraggeber, indem sie ihm IT-Infrastruktur, IT-Dienstleistung oder Software zur Verfügung stellt.

Des Weiteren findet beim Cloud Computing eine Auftragsdatenbearbeitung statt. Mit der Nutzung von Cloud Services werden Daten bearbeitet. Genau diese Datenbearbeitung ist Sinn und Zweck der Auslagerung – Daten sollen in der Cloud gespeichert und damit von überall zugänglich sein. Somit kommen beim Cloud Computing insbesondere die Vorschriften des Datenschutzrechts zur Anwendung.[8]

Die Nutzung von Cloud Services birgt – anders als andere Auslagerungen – höhere Risiken in sich. So besteht die Gefahr, dass Rahmenbedingungen der Auslagerung insgesamt und im Besonderen bei der Bearbeitung von Personendaten Persönlichkeitsrechte und Grundrechte verletzt werden können. Dies ist bei der Ausgestaltung zu berücksichtigen.[9]

Der Auftraggeber bleibt in jedem Fall für die ausgelagerte Tätigkeit bzw. Datenbearbeitung verantwortlich. Entsprechend sind in Achtung der rechtlichen Vorgaben sowie im Rahmen der Risikoanalyse weitere Abklärungen vorzunehmen und zusätzliche Überlegungen anzustellen. Es sind sowohl bei der Auswahl der Anbieterin, bei der Vertragsausgestaltung wie auch bei der Umsetzung von angemessenen organisatorischen und technischen Massnahmen die Herausforderungen bezüglich Transparenz, Kontrolle und Wahrnehmung der Verantwortung zusätzliche Punkte zu beachten.

Schliesslich stellen sich bei der Auslagerung in eine Cloud neben beschaffungsrechtlichen auch strategische und politische Fragen sowie Fragen des Vertragsmanagements. Der Entscheidung, eine Cloud-Lösung beizuziehen, gehen strategische Überlegungen voran. Die Beschaffung einer Cloud-Lösung muss den üblichen Beschaffungsprozess durchlaufen und dabei alle juristischen Anforderungen einbeziehen. Dafür sind schliesslich Verträge abzuschliessen. Dabei sind die Verhandlungen zwischen Auftraggeber und Auftragnehmerin durchzuführen, die Verträge zu implementieren und durchzusetzen sowie bei Bedarf Vertragsanpassungen vorzunehmen.

Dies Themen werden in der Arbeit sowohl in Kapitel 3. Auslagerung beim Staat als insbesondere auch in Kapitel 4. Auftragsdatenbearbeitung vertieft und fliessen schliesslich in die Handlungsanleitung in Kapitel 5 ein.

---

[8] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Merkblatt Cloud Computing, V 1.6 / Juli 2022, S. 1, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf> (zuletzt besucht am 29.04.2023).

[9] PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, V 3.0 / 03.02.2022, S. 2, abrufbar unter: <https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf> (zuletzt besucht am 29.04.2023).

3. Auslagerung beim Staat

Einleitend ist aus terminologischer Sicht festzuhalten, dass der Begriff «Auslagerung» unterschiedlich verwendet wird. Es kann damit jede Form von Beizug einer oder eines Dritten oder Übertragung auf eine oder einen Dritten gemeint sein. Bei diesem Verständnis fallen unter den Begriff Auslagerung die Organisationsprivatisierung (Übertragung von Verwaltungsaufgaben auf privatrechtlich organisierte Verwaltungsträger des Gemeinwesens, z.B. Swisscom), die Erfüllungsprivatisierung (Übertragung von Verwaltungsaufgaben auf Private, z.B. Electrosuisse), die Vermögensprivatisierung (Veräusserung staatlichen Eigentums an Private, z.B. Verkauf von Liegenschaften), die Finanzierungsprivatisierung (Einbezug von Privaten in die Finanzierung öffentlicher Aufgaben, z.B. Grundeigentümerbeiträge für Erschliessungen) und die Aufgabenprivatisierung (Verzicht auf staatliche Aufgabenerfüllung, z.B. Aufhebung einer landwirtschaftlichen Schule). Dabei wird auch die Verantwortung für die Aufgabenerfüllung übertragen. Ein anderes Verständnis fasst unter Auslagerung einzig den Beizug für eine Aufgabe oder die Übertragung einer Aufgabe auf eine oder einen Dritten zusammen, wobei die Verantwortung beim Auftraggeber verbleibt. In dieser Arbeit wird gemäss letzterem Verständnis vorgegangen.

3.1. Was den Staat zum Staat macht

In den folgenden Abschnitten wird aufgezeigt, was den Staat zum Staat macht. Daraus lassen sich die Unterschiede zu Privaten darlegen. Diese Unterschiede haben – wie bei jedem Handeln – natürlich auch bei der Auslagerung eine grosse Bedeutung.

3.1.1. Einteilung des Rechtsstoffs

Das Recht wird in der Schweiz grundlegend in zwei Rechtsgebiete unterteilt: Privatrecht und öffentliches Recht. Diese Unterteilung zeigt zwei völlig unterschiedliche Systeme auf. Das Privatrecht regelt die Beziehungen der Menschen untereinander, das öffentliche Recht beschäftigt sich mit dem Rechtsverhältnis zwischen dem Staat und den Bürgerinnen und Bürgern. Wichtigster Unterschied dieser Verhältnisse ist, dass sich die Partner im Privatrecht frei und gleichgestellt gegenüberstehen, während im öffentlichen Recht eine Unter- und Überordnung der Beteiligten besteht. Somit befasst sich das öffentliche Recht mit hoheitlicher Tätigkeit des Staates. Im römischen Recht wurde diese Unterscheidung wie folgt festgehalten: «Publicum jus est, quod ad statum rei publicae Romanae spectat, privatum, quod ad singulorum utilitatem»[10] («Öffentliches Recht ist das, was zum Staat hin ausgerichtet ist, Privatrecht dasjenige, was auf den Vorteil der Einzelnen gerichtet ist»).[11]

[10] Digesten 1, 1, 1, 2 (Ulpian).

[11] PETER FORSTMOSER/HANS-UELI VOGT, Einführung in das Recht, 5. Aufl., Stämpfli 2012, § 4 Rn. 44 ff.; AXEL TSCHENTSCHER/ANDREAS LIENHARD/FRANZISKA SPRECHER, Öffentliches Recht. Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., Dike 2019, Rn. 1.

3.1.2. Definition des Staates

Der Staat wird definiert als «der mit höchster Herrschaft ausgestattete Verband eines Volkes auf einem bestimmten Gebiet». Damit setzt sich der Staatsbegriff aus drei Elementen zusammen: Staatsvolk, Staatsgebiet, Staatsgewalt. Sind diese Elemente alle vorhanden, hat der Staat selbstständige, höchste Staatsgewalt. Diese umfasst die Rechtsetzung, die Verwaltung und die Justiz. Damit kann der Staat Vorschriften erlassen (Legislative), zur Aufgabenerfüllung hat er eine öffentliche Verwaltung, die von der Regierung angeleitet wird (Exekutive), und für die Rechtsdurchsetzung bestehen staatliche Gerichte (Judikative).[12]

3.1.3. Stellung des Staates

Die Stellung des Staates unterscheidet sich damit stark von jener der Einzelnen untereinander. Es besteht ein Machtgefälle, der Staat hat eine stärkere Stellung und kann gegenüber der Bevölkerung dominant auftreten. In dieser Konstellation haben die Bürgerinnen und Bürger keine Wahlmöglichkeit – sie müssen mit der jeweils zuständigen staatlichen Institution interagieren. Es besteht auch keine Freiwilligkeit – gegenüber dem Staat sind Pflichten zu erfüllen und die Rechte stehen der Bevölkerung zu.

3.1.4. Verfassungsmässige Prinzipien

Die Verfassung gibt dem Staat Prinzipen vor, nach denen er sein Handeln auszurichten hat. Dazu gehören unterschiedliche Leitlinien wie insbesondere auch die Grundrechte. Daraus entsteht ein Gleichgewicht indem der Staat einerseits eingreifend seine Aufgaben (wie beispielsweise den Einzug von Steuern) zu erfüllen hat und andererseits durch verfassungsmässige Vorgaben (wie beispielsweise den Verhältnismässigkeitsgrundsatz) gesteuert wird, so dass die Rechte der Bürgerinnen und Bürger gewahrt werden. Diese Vorgaben definieren die Rechtsstellung der Bürgerinnen und Bürger und garantieren, dass sich der Staat aufgrund des vorliegenden Unter- und Überordnungsverhältnis, das ihm weite Befugnisse gibt, in einem engen und klar definierten Rahmen bewegt.[13]

Zu den wichtigsten verfassungsmässigen Vorgaben gehören:[14]

- **Demokratie** (Präambel und Art. 2 BV[15]): Rechtssetzungsprozesse erfolgen gemäss demokratischen Grundsätzen, die Bevölkerung hat dabei demokratische Mitwirkungsrechte.
- **Rechtsstaatlichkeit und Legalitätsprinzip** (Art. 5 Abs. 1 und Art. 36 Abs. 1 BV): Grundlage und Schranke staatlichen Handelns ist das Recht. Damit ist das staatliche Handeln vo-

---

[12] ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER/DANIELA THURNHERR, Schweizerisches Bundesstaatsrecht, 10. Aufl., Schulthess 2020, Rn. 930 ff.; ARTHUR BENZ, Der moderne Staat. Grundlagen der politologischen Analyse, 2. Aufl., De Gruyter 2008, S. 38.

[13] TOBIAS JAAG/LAURA BUCHER/RETO HÄGGI FURRER, Staatsrecht der Schweiz. in a nutshell, 2. Aufl., Dike 2016, S. 2.

[14] ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER/DANIELA THURNHERR, Schweizerisches Bundesstaatsrecht, 10. Aufl., Schulthess 2020, Rn. 168 ff.; TOBIAS JAAG/LAURA BUCHER/RETO HÄGGI FURRER, Staatsrecht der Schweiz. in a nutshell, 2. Aufl., Dike 2016, S. 3 ff.

[15] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV), SR 101.

raussehbar, es dient der Rechtssicherheit und gewährleistet eine rechtsgleiche Behandlung der Bürgerinnen und Bürger. Bürgerinnen und Bürger sind vor Willkür geschützt.

- **Öffentliches Interesse** (Art. 5 Abs. 2 und Art. 36 Abs. 2 BV): Staatliches Handeln muss im Interesse der Allgemeinheit liegen.
- **Verhältnismässigkeitsgrundsatz** (Art. 5 Abs. 2 und Art. 36 Abs. 3 BV): Staatliches Handeln muss geeignet und erforderlich zur Aufgabenerfüllung sein sowie in einem vernünftigen Verhältnis stehen.
- **Treu und Glauben** (Art. 5 Abs. 3 BV): Es gilt das Verbot des Rechtsmissbrauchs sowie das Verbot des widersprüchlichen Verhaltens.
- **Gewaltenteilung**: Staatliche Macht wird auf drei sich hemmende und getrennte Gewalten verteilt, die damit kontrolliert werden: Legislative, Exekutive und Judikative.
- **Grundrechte** (Art. 7 – 35 BV): Den Bürgerinnen und Bürgern stehen Grundrechte zu.
- **Bundesstaatlichkeit**: Die Kompetenzbereiche sind auf drei staatliche Ebenen (Bund, Kantone, Gemeinden) verteilt.
- **Sozialstaatlichkeit**: Die Bundesverfassung hält Sozialziele (Art. 41 BV) und soziale Grundrechte (Recht auf Hilfe in Notlagen (Art. 12 BV), Anspruch auf unentgeltlichen Grundschulunterricht (Art. 19 BV), teilweise Anspruch auf unentgeltliche Rechtspflege und Rechtsbeistand (Art. 29 Abs. 3 BV)) fest.
- **Nachhaltigkeit** (Präambel, Art. 2 Abs. 2 und 4, Art. 73 BV): Bund und Kantone sind zur Nachhaltigkeit verpflichtet. Damit soll eine nachhaltige Entwicklung in allen Bereichen gewährleistet und so die Verantwortung gegenüber nachfolgenden Generationen wahrgenommen werden.
- **Subsidiarität** (Art. 5a BV): Der Staat erfüllt jene Aufgaben, die das Individuum nicht selber erfüllen kann. Der Bund nimmt nur Aufgaben wahr, die die Kantone nicht zufriedenstellend erfüllen können.

Aus diesen Verfassungsgrundsätzen zeigt sich die besondere Verantwortung, die der Staat in seiner Aufgabenerfüllung gegenüber der Bevölkerung hat. Die Grundsätze geben ihm entsprechend den Rahmen vor. Im Vordergrund steht dabei das Legalitätsprinzip: Jedes staatliche Handeln braucht eine Rechtsgrundlage. Dabei ist eine Einwilligung von Bürgerinnen und Bürgern in staatliche Tätigkeiten nicht möglich.

Der Staat hat sich insbesondere an die Grundrechte zu halten. Das heisst, wenn er in Grundrechte eingreifen möchte oder muss, kann er dies nur tun, wenn dafür eine Rechtsgrundlage besteht, der Eingriff im öffentlichen Interesse liegt und verhältnismässig ist (Art. 36 Abs. 1-3 BV). Zudem darf er den Kerngehalt der Grundrechte nicht tangieren (Art. 36 Abs. 4 BV). Private müssen sich im Privatrechtsverkehr grundsätzlich nicht an die Grundrechte halten. Einzelne Grundrechte haben eine direkte Wirkung, indem sie doch auch zwischen Privaten gelten (z.B. Lohngleichheit zwischen Frau und Mann). Der Staat ist aufgrund seiner Schutzpflicht zudem aber auch verpflichtet, die Grundrechte in der Rechtsordnung insgesamt – also in einem gewissen Sinne auch im Verhältnis zwischen Privaten – umzusetzen. Das geschieht, indem die Grundrechte bei der Rechtsetzung allgemein einbezogen werden.

3.1.5. Unterscheidung zu privaten Akteuren

Zusammenfassend können folgende Unterschiede zwischen Rechtsbeziehungen von Privaten untereinander und der Rechtsbeziehung des Staates zur Bevölkerung festgehalten werden:

- In der Rechtsbeziehung zwischen dem Staat und Individuen besteht ein **Unter-/Überordnungsverhältnis**, ein Machtgefälle. Private sind gleichgestellt.
- Für den Staat gilt das **Legalitätsprinzip**. Private können ohne rechtliche Grundlage frei Vereinbarungen treffen. Entsprechend können sie gestützt auf Einwilligungen Verpflichtungen eingehen.
- Der Staat muss sich an die **Grundrechte** halten. Private haben diese Pflicht nur beschränkt bzw. nicht umfassend.
- Bei Beziehungen zum Staat besteht meist ein **Zwang**, während privatrechtliche Beziehungen in der Regel freiwillig entstehen.
- In der Beziehung zum Staat sind die Bürgerinnen und Bürger an eine bestimmte staatliche Institution **gebunden**. Unter Privaten herrscht Wahlfreiheit.

Aus diesen wesentlichen Unterschieden ergibt sich für den Staat eine grosse **Verantwortung** gegenüber den Individuen. Diese muss er sich bei seinen Handlungen bewusst sein und hat sich entsprechend an die Vorgaben zu halten.

3.2. Staatliche Aufgabenerfüllung

Im oben umschriebenen Rahmen kommen dem Staat bestimmte Aufgaben zu. Diese werden ihm zugeteilt und in Gesetzen umschrieben. Der Staat ist bei der Aufgabenerfüllung insbesondere an die verfassungsmässigen Prinzipien gebunden.

In den folgenden Abschnitten werden die staatlichen Aufgaben definiert, ihre Arten sowie die Art und Weise deren Erfüllung umschrieben.

3.2.1. Definition von staatlichen Aufgaben

Staatsaufgaben sind Aufgaben, die dem Staat mittels eines demokratischen Prozesses zugewiesen wurden. Im Ergebnis regeln die Gesetze die Aufgaben des Staates und auch, wie er diese zu erfüllen hat. Dies betrifft insbesondere die Art und Weise, die Form, die Zeit und die Organisation. Der Staat besorgt diese Verwaltungsaufgaben unter Einhaltung des gesetzlich festgehaltenen Rahmens. Er erfüllt diese Aufgaben grundsätzlich selber.[16]

Inhaltlich umfassen die staatlichen Aufgaben beispielsweise folgende Themenfelder:

- Schaffung und Erhaltung eines Rechtsrahmens (Gesetzgebung, Gerichte)
- Gewährleistung der inneren und äusseren Sicherheit (Polizeiaufgaben, Militär)
- Finanzen (Steuern, Subventionen)

[16] AXEL TSCHENTSCHER/ANDREAS LIENHARD/FRANZISKA SPRECHER, Öffentliches Recht. Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., Dike 2019, Rn. 355.

- Sicherstellung einer Infrastruktur (Verkehr, Abwasser, Stromversorgung, Kommunikation)
- Verbraucherschutz und Wirtschaft
- Raumplanung, Umwelt-, Natur- und Heimatschutz
- Bildung und Forschung
- Gesundheit
- Soziale Sicherheit

3.2.2. Arten von staatlichen Aufgaben

Es gibt unterschiedliche staatliche Aufgaben, die unterschiedliche Ziele verfolgen und unterschiedliche Zwecke erfüllen. Die verschiedenen Verwaltungsaufgaben lassen sich wie folgt einteilen:[17]

- **Ordnungsaufgaben**: Stellen Zustand her und schützen vor Störungen und werden mittels Eingriffsverwaltung erfüllt.
- **Sozialpolitische Aufgaben**: Bewirken einen Ausgleich von Benachteiligungen gewisser Gesellschaftsgruppen oder Individuen und werden mittels Leistungsverwaltung oder Eingriffsverwaltung erfüllt.
- **Lenkungsaufgaben**: Sollen in eine bestimmte Richtung führen und werden durch Leistungs- und Eingriffsverwaltung erfüllt.
- **Infrastrukturaufgaben**: Stellen den Service public sicher.

3.2.3. Arten der staatlichen Aufgabenerfüllung

Aus den staatlichen Aufgaben ergeben sich unterschiedliche Arten der Aufgabenerfüllung durch den Staat. So wird zunächst zwischen Eingriffs- und Leistungsverwaltung unterschieden. Bei der Eingriffsverwaltung greift der Staat in Rechte und Freiheiten der Einzelnen ein oder beschränkt diese, indem er beispielsweise Verbote vorsieht. Damit auferlegt er den Bürgerinnen und Bürgern Verpflichtungen oder Belastungen. Bei der Leistungsverwaltung werden Individuen begünstigt, indem ihnen eine staatliche Leistung – i.S.v. Vorteilen oder Vergünstigungen – vermittelt wird.[18]

Zudem erfüllt der Staat seine Aufgaben mittels Bedarfsverwaltung. Diese sorgt für die Bereitstellung von Personal- und Sachmitteln, die für die Aufgabenerfüllung benötigt werden. Dazu zählt insbesondere das Beschaffungswesen, das dem Staat Vorgaben macht zur Art und Weise, wie Waren oder Dienstleistungen eingekauft werden können.[19]

---

[17] PIERRE TSCHANNEN/ULRICH ZIMMERLI/MARKUS MÜLLER, Allgemeines Verwaltungsrecht, 4. Aufl., Stämpfli 2014, § 3 Rn. 1 ff.; AXEL TSCHENTSCHER/ANDREAS LIENHARD/FRANZISKA SPRECHER, Öffentliches Recht. Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., Dike 2019, Rn. 388 ff.

[18] PIERRE TSCHANNEN/ULRICH ZIMMERLI/MARKUS MÜLLER, Allgemeines Verwaltungsrecht, 4. Aufl., Stämpfli 2014, § 4 Rn. 3 ff.

[19] PIERRE TSCHANNEN/ULRICH ZIMMERLI/MARKUS MÜLLER, Allgemeines Verwaltungsrecht, 4. Aufl., Stämpfli 2014, § 4 Rn. 8 ff.

3.3. Auslagerung von staatlichen Aufgaben

Nicht alle Aufgaben des Staates sind zwingend durch den Staat selber zu erfüllen. Je nach Aufgabe können in unterschiedlicher Art und Weise Dritte beigezogen oder Aufgaben auf Dritte übertragen werden. Gleichzeitig gibt es Aufgaben, die zwingend durch den Staat zu erfüllen sind und nicht weitergegeben werden können.

Nach der Auslagerungsfähigkeit der Aufgaben können folgende Typen der Verwaltungsaufgaben unterschieden werden:[20]

- **Ministerialaufgaben**: Aufgaben, die die Politikvorbereitung betreffen und Verwaltungstätigkeiten mit hoheitlichem Charakter, die häufig mit Grundrechtseingriffen verbunden sind. *Auslagerungsfähigkeit fehlt, z.B. Polizeitätigkeit*
- **Monopoldienstleistungen**: Grundzüge werden durch die Politik bestimmt, ansonsten Autonomie erforderlich. *Auslagerungsfähig, z.B. durch öffentlich-rechtliche Anstalten*.
- **Marktaufsicht**: Bedürfen der Unabhängigkeit. *Auslagerung sinnvoll, z.B. Anstalt oder Behördenkommission.*
- **Dienstleistungen am Markt**: Bedürfen einer grossen Autonomie. *Müssen ausgelagert werden, z.B. spezialgesetzliche oder privatrechtliche Aktiengesellschaft.*

Es stellt sich also zunächst die Frage, ob eine Aufgabenerfüllung überhaupt für eine Auslagerung geeignet ist. So sind beispielsweise Ministerialaufgaben nicht zur Auslagerung geeignet. Dienstleitungen, die am Markt erbracht werden, sollen hingegen ausgelagert werden, damit eine Positionierung auf dem Markt überhaupt möglich ist.

Ist die Auslagerungsfähigkeit zu bejahen, stellt sich weiter die Frage, wie die Übertragung erfolgen soll bzw. wie diese Auslagerung geregelt werden kann. Es gibt dafür verschiedene Vorgehensweisen. So kann die Auslagerung (spezial-)gesetzlich vorgesehen sein. Sie kann aber auch mittels Leistungskontrakt übertragen werden. Damit wird eine öffentliche Aufgabe im Bereich des Subventionsrechts mittels Abgeltungen erfüllt. Mit der Public Corporate Governance werden Grundsätze zur Organisation und Steuerung umschrieben, die bei der Auslagerung von Aufgabenerfüllungen wirksame und effiziente Leistungserbringung im demokratischen Rechtsstaat sicherstellen sollen.

3.4. Beschaffungswesen

Die hier diskutierte Auslagerung betrifft IT-Dienstleistungen. Die staatliche Tätigkeit soll durch den Beizug von IT-Infrastruktur und Cloud-Lösungen unterstützt werden. Werden IT-Dienstleistungen eingekauft, ist für öffentliche Institutionen vorgeschrieben, dass diese finanziellen Ausgaben nach einem bestimmten Ablauf und unter Berücksichtigung von bestimmten Kriterien getätigt werden.

---

[20] AXEL TSCHENTSCHER/ANDREAS LIENHARD/FRANZISKA SPRECHER, Öffentliches Recht. Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., Dike 2019, Rn. 393 ff.

Nachdem die rechtlichen Grundlagen festgehalten werden, werden in den folgenden Abschnitten der Ablauf einer Beschaffung dargestellt sowie die konkreten Implikationen für die Beschaffung von IT-Dienstleistungen erörtert.

3.4.1. Rechtsgrundlagen

Die Vorgaben für den Beschaffungsprozess sind für Bundesorgane im Bundesgesetz über das öffentliche Beschaffungswesen sowie den dazu gehörigen Ausführungsbestimmungen in Verordnungen festgehalten.[21]

Die Regelung des Beschaffungswesens für kantonale Institutionen liegt in der Kompetenz der Kantone. Damit die internationalen Vorgaben (WTO-GPA[22]) gesamtschweizerisch eingehalten werden können, haben die Kantone die Interkantonale Vereinbarung über das öffentliche Beschaffungswesen (IVöB)[23] erlassen. Die IVöB stellt eine gemeinsame Rahmenordnung dar, um die Umsetzung des WTO-GPA auf kantonaler Ebene zu erleichtern.

In diesem Zusammenhang wird eine gemeinsame elektronische Plattform von Bund, Kantonen und Gemeinden im Bereich des öffentlichen Beschaffungswesens (simap.ch) durch das Staatssekretariat für Wirtschaft (Seco) betrieben und vom Verein simap.ch verantwortet. Sie dient der Veröffentlichung von Ausschreibungen von öffentlichen Auftraggebern.

3.4.2. Vorgehen

Bei der Beschaffung wird nach einem geregelten Zyklus vorgegangen. Der Beschaffungszyklus startet mit der Bedarfserkennung. Dieser Bedarf wird sodann definiert (Planungsphase). Gestützt auf die Bedarfsdefinition kann die Ausschreibung erfolgen. In diesem Schritt ist es besonders wichtig, alle Bedürfnisse und damit auch Vorgaben, die staatliche Institutionen einzuhalten haben, in der Ausschreibung festzuhalten. Nur so können staatliche Institutionen ihre Verpflichtungen wahrnehmen und somit rechtmässig beschaffen. Als Abschluss des Ausschreibungsprozesses wird dem vorteilhaftesten Angebot der Zuschlag erteilt (Art. 41 BöB; Vergabephase). Es folgt die Phase der Vertragserfüllung und schliesslich kommt es nach Ablauf einer gewissen Zeit zum «End of Life» bzw. Vertragsende (Vertragsphase).

Während des gesamten Beschaffungszyklus sind die Prinzipien des Beschaffungsrechts einzuhalten (Art. 2 BöB): Dazu gehören insbesondere die Grundsätze der Nachhaltigkeit (ökologische, ökonomische und soziale Nachhaltigkeit), der Transparenz (Publikationspflicht, Begründungspflicht) und des Wettbewerbs (Gleichbehandlungsgebot, Diskriminierungsverbot).

Dieses Vorgehen stellt einen Unterschied zur Privatwirtschaft dar, die unabhängig von solchen Vorgaben beispielsweise IT-Dienstleitungen anschaffen kann.

---

[21] Bundesgesetz über das öffentliche Beschaffungswesen vom 21. Juni 2019 (BöB), SR 172.056.1; Verordnung über das öffentliche Beschaffungswesen vom 12. Februar 2020 (VöB), SR 172.056.11; Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung vom 24. Oktober 2012 (Org-VöB), SR 172.056.15.

[22] Revidiertes Übereinkommen über das öffentliche Beschaffungswesen vom 15. April 1994 (WTO-GPA), SR 0.632.231.422.

[23] Interkantonale Vereinbarung über das öffentliche Beschaffungswesen vom 15. März 2001 (IVöB).

Dieser Beschaffungszyklus lässt sich graphisch wie folgt darstellen:

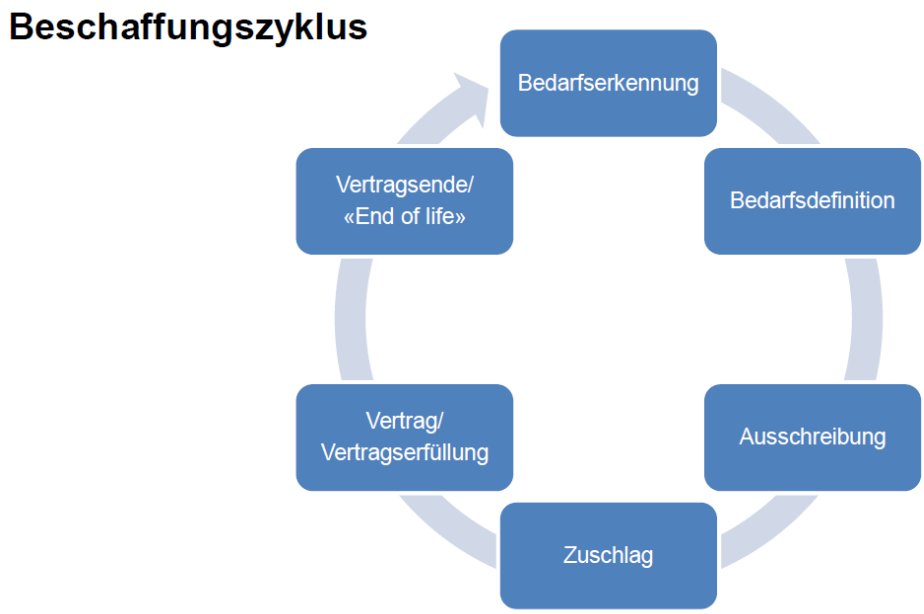

Abbildung 3: Beschaffungszyklus[24]

3.4.3. Beschaffung von IT-Dienstleistungen

Will der Staat IT-Dienstleistungen wie beispielsweise Cloud-Lösungen einsetzen und diese nicht selber erstellen, wird er im Rahmen der Auslagerung und damit im Beschaffungsprozess eine Ausschreibung für diese Dienstleistung publizieren. Dabei ist besonders zu berücksichtigen, dass öffentliche Institutionen an die verfassungsmässigen Prinzipien gebunden sind, die zudem in den gesetzlichen Bestimmungen zum Beschaffungswesen konkretisiert sind. Aus diesem Grund haben öffentliche Institutionen bei der Bedarfsdefinition auf die beispielsweise sich aus den datenschutzrechtlichen Bestimmungen ergebenden Vorgaben besonderes Augenmerk zu richten. Denn wenn sie diese nicht bereits bei der Beschaffung umsetzen, wird eine spätere Umsetzung sehr aufwändig wenn nicht gar unmöglich. Damit würde die öffentliche Institution Verfassungsrecht bzw. gesetzliche Vorgaben verletzen.

Diese Überlegungen sind auch bei Cloud-Lösungen einzubeziehen. Im Kapitel zur Auftragsdatenbearbeitung weiter unten werden die Vorgaben zu Cloud-Lösungen ausgearbeitet bzw. festgehalten. Die öffentliche Institution hat diese bereits in der Ausschreibung als verbindlich anzugeben.

Im Rahmen der Planungsphase haben sich öffentliche Institutionen mit Fragen zu beschäftigen, wie beispielsweise: Welche Anbieterinnen gibt es? Welche Eigenschaften haben diese? Welche Dienstleistungen bieten sie an? Bearbeitet die IT-Lösung Personendaten? Welche und wie? Welche technischen Massnahmen sind erforderlich? Muss die Dienstleisterin eine Zertifizierung ausweisen?

---

[24] RIKA KOCH, Implementierung datenschutzrechtlicher Anforderungen im öffentlichen Beschaffungsprozess, Referat am Schulthess Forum Datenschutz in Städten und Gemeinden, 3. März 2023, Folie 5.

In der Ausschreibung sind die Antworten auf diese Fragen festzuhalten und als zu erfüllende Kriterien vorauszusetzen. Beim Zuschlag müssen im Ergebnis Anbieterinnen ausgeschlossen werden, welche die (insbesondere auch datenschutzrechtlichen und -technischen) Vorgaben nicht erfüllen (können).

In der Vertragsphase sind schliesslich alle Vorgaben vertraglich mit der Anbieterin zu vereinbaren und die Umsetzung der erforderlichen technischen Massnahmen ist durch die öffentliche Institution zu überwachen.

3.5. Strategische Überlegungen bei der Auslagerung

Zu den staatsrechtlichen Überlegungen kommen strategische Überlegungen dazu. Die öffentliche Institution muss sicherstellen, dass sie ihre Aufgaben erfüllen kann – auch, wenn sie eine Dritte oder einen Dritten im Rahmen einer Auslagerung beizieht. Sie muss sich strategisch überlegen, welchen Einfluss der Beizug einer Dienstleisterin auf die Aufgabenerfüllung haben kann.

Eine Strategie verfolgt zunächst ein Ziel, einen Zweck.[25] Möchte die öffentliche Institution die aktuellen Entwicklungen beispielsweise zu New Work 4.0 mitmachen und ihren Mitarbeitenden ermöglichen, flexibel zu arbeiten, stellt sich die Frage, wie dieses Ziel erreicht werden kann bzw. welche Punkte bei der Planung einbezogen und berücksichtigt werden müssen. Welche Strategie führt am besten zum erklärten Ziel?

Dabei sind auch die Anspruchsgruppen[26], ganz konkret die Mitarbeitenden, einzubeziehen. Ist die Veränderung der Arbeitswelt und -weise in eine Digitalisierungsstrategie der öffentlichen Institution insgesamt eingebettet, gehört auch die Bevölkerung zu den Anspruchsgruppen. Hier ist zu evaluieren, welche Bedürfnisse bestehen, welche Möglichkeiten (wie z.B. Tools) vorhanden sind wie auch welche Entwicklungen zu erwarten sind.

Weiter stellen sich Fragen zu Ressourcen und Kompetenzen[27] der öffentlichen Institution. Hat sie die notwendigen Ressourcen und insbesondere auch die notwendigen Kompetenzen und das Know-How, um das strategische Ziel zu erreichen? Kann die öffentliche Institution beispielsweise selbst eine Cloud-Lösung zur Verfügung stellen, die die eruierten Bedürfnisse abdeckt?

Gestützt darauf soll die Wertschöpfung mit Prozessen und Strukturen organisiert werden und den Mitarbeitenden bzw. der Bevölkerung ein Mehrwert, ein Kundennutzen, letztlich als Gemeinwohlbeitrag, entstehen.

Diese Gedanken entlang der Themengebiete lassen sich graphisch im Strategiedreieck wie folgt darstellen:

---

[25] GERRY JOHNSON/RICHARD WHITTINGTON/KEVAN SCHOLES/DUNCAN ANGWIN/PATRICK REGNÉR, Strategisches Management. Eine Einführung, 11. Aufl., Pearson 2018, S. 29 f.

[26] GERRY JOHNSON/RICHARD WHITTINGTON/KEVAN SCHOLES/DUNCAN ANGWIN/PATRICK REGNÉR, Strategisches Management. Eine Einführung, 11. Aufl., Pearson 2018, S. 181 ff.

[27] GERRY JOHNSON/RICHARD WHITTINGTON/KEVAN SCHOLES/DUNCAN ANGWIN/PATRICK REGNÉR, Strategisches Management. Eine Einführung, 11. Aufl., Pearson 2018, S. 138 ff.

Abbildung 4: Strategiedreieck[28]

Zu den strategischen Überlegungen im Rahmen einer Auslagerung von IT-Dienstleistungen und insbesondere die Nutzung einer Cloud-Lösung gehören ganz konkret die folgenden Themen:

- Kontrollverlust: Werden staatliche Aufgaben wie beispielsweise Datenbearbeitungen in einer Cloud ausgelagert, kann dies zum Verlust der Kontrolle über diese Daten führen.
- Datensouveränität: Mit dem Beizug einer Cloud-Anbieterin wird die Datensouveränität in Frage gestellt. Es stellen sich Fragen, wo die Daten gespeichert sind und damit welchem Recht sie unterliegen und ob dieses mit lokalen Vorgaben vereinbar ist. Zudem ist unklar, wer auf die Daten zugreifen kann.
- Risikomanagement: Je nach Datenbearbeitung kann eine Auslagerung dazu führen, dass Risiken verringert werden können oder auch, dass die Risiken steigen.
- Informationssicherheit: Es ist zu prüfen, ob Cloud-Anbieterinnen die erforderliche Informationssicherheit sicherstellen können.
- Lock-In-Effekte: Welchen Einfluss hat ein System-Lock-In (d.h. eine technische Abhängigkeit, z.B. bezüglich Schnittstellen, oder eine organisatorische Abhängigkeit, z.B. bezüglich Gewohnheiten von Mitarbeitenden)? Welchen Einfluss kann ein Vender-Lock-In (d.h. eine rechtliche Abhängigkeit, z.B. bezüglich Verträgen oder Lizenzen, oder Know-How-Abhängigkeiten, z.B. wenn Mitarbeitende die Abläufe nicht mehr kennen, weil das Know-

[28] CLAUS JACOBS, Strategisches Management in öffentlichen Organisationen. Strategiearbeit in öffentlichen Organisationen, Unterricht am eMPA, 10. Mai 2022, Folie 9.

How ausgelagert wird, oder auch psychologische Abhängigkeiten, wie z.B. bekannte Marken usw.) haben? Mit dem Entscheid für eine Cloud-Anbieterin entsteht zweifellos eine grosse Abhängigkeit. Wechsel zu anderen Anbieterinnen kann so erschwert oder nicht möglich sein. Gilt es dies zu vermeiden?

- Kostenersparnis: Auslagerung kann kostensparend sein, je nachdem aber auch nicht.
- Skalierbarkeit: Cloud-Angebote ermöglichen den skalierbaren Bezug von Speicherkapazitäten. Damit können diesbezüglich kurzfristig Anpassungen vorgenommen werden.
- Bessere Produkte aufgrund der Expertise von Dienstleisterinnen: Wenn externe Dienstleisterinnen beigezogen werden, kann deren besondere Expertise eingebracht werden, die je nachdem bei der öffentlichen Institution nicht vorhanden ist.
- Örtliche Flexibilität für die Aufgabenerfüllung: Mitarbeitende können von überall her auf die Daten zugreifen und auch so ihrer Arbeit nachgehen.
- Nachhaltigkeit: Wie kann mit dem Beizug einer IT-Dienstleistung die Nachhaltigkeit sichergestellt werden?
- Öffentliche Wahrnehmung: Wie nimmt die Öffentlichkeit und auch die Politik die Auslagerung wahr? Akzeptiert sie den Kontrollverlust? Wie schätzt sie die Rechtmässigkeit der Auslagerung ein? Gehen damit Arbeitsplätze verloren?
- Qualitätsverlust: Die Arbeitsweise kann erschwert sein, wenn bei der Anbieterin beispielsweise technische Schwierigkeiten entstehen. Führt eine gute Dienstleistung der Anbieterin zu besserer Qualität der Aufgabenerfüllung?

Diese strategischen Überlegungen zeigen auf, dass die Auslagerung und der Einsatz einer Cloud-Lösung potentiell viele Vor- aber auch Nachteile haben kann. Daher sind diese sorgfältig gegen einander abzuwägen. So kann mit der Auslagerung eine Kostenersparnis wie auch die Möglichkeit, nicht vorhandene Expertise beizuziehen, mehr Informationssicherheit, Skalierbarkeit und Flexibilität erlangt werden. Gleichzeitig erfolgt ein Kontroll- und Transparenzverlust. Zudem ist die Datensouveränität in Frage gestellt. Lock-In-Effekte schränken die Freiheit ein und führen zu einer bedeutenden Abhängigkeit der staatlichen Institutionen von privaten Anbieterinnen.

Im Ergebnis stellt sich die vielfach diskutierte – und bedauerlicherweise immer wieder verworfene – Frage, ob eine staatliche Cloud erstellt werden könnte (z.B. als Community Cloud). Eine solche, beispielsweise durch den Bund betriebene, Cloud könnte die offenen Fragen klären bzw. die bestehenden Risiken wesentlich einschränken. Insbesondere würde keine Abhängigkeit entstehen, es würde kein Kontrollverlust entstehen und die öffentlichen Institutionen in der Schweiz könnten die Dienste rechtskonform nutzen.

3.6. Politische Überlegungen bei der Auslagerung

Die politischen Akteure sind neben juristischen und strategischen Überlegungen auch einzubeziehen. So entstehen Gesetze gerade in einem politischen Prozess, der sie legitimiert. Auf dieser Ebene können die wesentlichen Entscheide gefällt werden. Entsprechend hat die Politik einen grossen Einfluss auf die Entscheidfindung.

Das trifft zunächst auf die Parlamente aller staatlichen Stufen (Bund, Kantone, Gemeinden) zu. Die Parlamentarier bringen Anliegen ein und können so einen Gesetzgebungs- oder anpassungsprozess anstossen. Oder sie gestalten den Gesetzgebungsprozess in der Debatte mit.

Des Weiteren haben die Regierungen aller staatlichen Ebenen (Bund, Kantone, Gemeinden) die Möglichkeit, beispielsweise in der Legislaturplanung Strategien – wie beispielsweise Digitalisierungsstrategien – zu verabschieden. Sie gestalten damit die Entwicklungen in ihren jeweiligen Institutionen mit und geben diese vor.

Nicht zuletzt hat auch das Volk ein Mitspracherecht und kann sich mit unterschiedlichen Instrumenten (z.B. Volksinitiative, Referendum) einbringen und mitgestalten.

Diese Einflüsse sind bei der Auslagerung zu berücksichtigen. So kann insbesondere eine Auslagerung auf diese Art und Weise vorgeschlagen und angestossen oder auch verhindert werden.

4. Auftragsdatenbearbeitung

Wird eine Aufgabe ausgelagert, findet meist auch eine Datenbearbeitung statt. So werden beim Auftrag, ein Gutachten zu verfassen, eine Weiterbildungsveranstaltung durchzuführen, ein Coaching für Mitarbeitende anzubieten wie auch beim Betrieb einer IT-Infrastruktur immer auch Daten bearbeitet. Der Auftraggeber überträgt somit zeitgleich jeweils auch eine Datenbearbeitung an die Auftragnehmerin.[29] Damit sind neben den allgemeinen oben beschriebenen Auslagerungsvorgaben auch datenschutzrechtliche und -technische Vorgaben für die Auslagerung einer Datenbearbeitung einzuhalten.

Terminologisch wird hier unter Auslagerung Outsourcing verstanden, bei dem eine Dritte oder ein Dritter bei der staatlichen Aufgabenerfüllung beigezogen wird oder die Aufgaben auf sie oder ihn übertragen wird. Dabei bleibt die Verantwortung für die Aufgabenerfüllung und damit auch für die Datenbearbeitung immer bei der öffentlichen Institution.

Beim Beizug von Cloud-Dienstleitungen findet immer auch eine Auslagerung einer Datenbearbeitung, eine Auftragsdatenbearbeitung, statt. Denn mit dem Einsatz von Cloud Computing werden Daten bearbeitet. Diese Auslagerung birgt – anders als andere Auslagerungen – höhere Risiken in sich. So besteht die Gefahr, dass Rahmenbedingungen der Auslagerung insgesamt und im Besonderen bei der Bearbeitung von Personendaten Persönlichkeitsrechte und Grundrechte verletzt werden können. Somit sind in Achtung der rechtlichen Vorgaben sowie im Rahmen der Risikoanalyse weitere Abklärungen vorzunehmen und zusätzliche Überlegungen anzustellen. Es sind sowohl bei der Auswahl der Anbieterin, bei der Vertragsausgestaltung wie auch bei der Umsetzung von angemessenen organisatorischen und technischen Massnahmen die Herausforderungen bezüglich Transparenz, Kontrolle und Wahrnehmung der Verantwortung zusätzliche Punkte zu beachten.[30]

Nachdem zunächst die Arten der Auftragsdatenbearbeitung aus datenschutzrechtlicher Perspektive dargelegt und abgegrenzt werden, wird geklärt, welches Datenschutzrecht anwendbar ist. Aus den rechtlichen Grundlagen ergeben sich die Voraussetzungen für die Auftragsdatenbearbeitung, die im Hauptteil anhand der Auslagerung einer Datenbearbeitung in eine Cloud behandelt werden. Dabei stellen sich insbesondere zwei Fragen: Darf ausgelagert werden? Wie ist auszulagern? Schliesslich wird das methodische Vorgehen aufgezeigt und das Spezialthema der Auslagerung mit Auslandbezug aufgenommen.

---

[29] VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 1.

[30] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Merkblatt Cloud Computing, V 1.6 / Juli 2022, S. 1, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf> (zuletzt besucht am 29.04.2023).

4.1. Arten der Auftragsdatenbearbeitung

Es können je nach Inhalt des Auftrags und der Art der bearbeiteten Daten verschiedene Arten der Auftragsdatenbearbeitung unterschieden werden:[31]

- **Inanspruchnahme von Informatikleistungen:** z.B. Betrieb und Wartung einer IT-Infrastruktur oder Software (Netzwerk, Server, Anwendungen), Hosting von Webangeboten und Services (Websites, Analysetools) oder die Inanspruchnahme von Cloud Services.
- **Datenbearbeitung durch Dritte:** Bei dieser Art der Auftragsdatenbearbeitung entsteht ein «Produkt» aus den Daten des Auftraggebers, z.B. Auftrag einer Gemeinde an ein Anwaltsbüro, einen Beschluss zu formulieren oder ein Gutachten zu einer bestimmten Fragestellung zu verfassen, oder auch ein Auftrag zur Durchführung von Bildungsprogrammen.
- **Inanspruchnahme von Dienstleistungen:** Bei dieser Art der Auftragsdatenbearbeitung erfolgt eine Dienstleistungen, die nicht ohne Informationen des Auftraggebers erbracht werden kann, deren Hauptinhalt jedoch Eigenleistungen der Auftragnehmerin sind und in deren Rahmen das Bearbeiten der Daten des Auftraggebers nicht Schwerpunkt ist, z.B. Coaching, Wartung von Geräten oder der Druck und Versand von Rechnungen.

Die Auftragsdatenbearbeitung ist von der selbstständigen Aufgabenerfüllung abzugrenzen.[32] Werden öffentliche Institutionen mit der Aufgabenerfüllung betraut, indem sie beispielsweise einen Leistungsauftrag haben (z.B. Spitäler mit kantonalem Leistungsauftrag gemäss Spitalliste) oder selbstständige öffentlich-rechtliche Anstalten sind (z.B. Universitätsspital), liegt keine Auslagerung vor. Diese Institutionen erfüllen in diesen Fällen die Aufgaben selbstständig.

Abzugrenzen ist die Auftragsdatenbearbeitung zudem von der Datenbekanntgabe. Eine Datenbekanntgabe liegt vor, wenn eine öffentliche Institution gestützt auf eine gesetzliche Grundlage einer dritten Person oder Organisation Informationen bekannt gibt, damit diese sie zu eigenen Zwecken bearbeiten kann.[33] Bei der Auslagerung findet keine Datenbekanntgabe statt. Die Verantwortung für die Datenbearbeitung verbleibt bei der öffentlichen Institution.

---

[31] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 2 ff., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

[32] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 6 f.; VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 29; DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 4, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

[33] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 10; VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 5; DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Leitfaden «Auftragsdatenbearbeitung» (Bearbeitenlassen von Personendaten durch Dritte, § 7 IDG), V 1.0 / 08.04.2016, S. 1, abrufbar unter: <https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html> (zuletzt besucht am 29.04.2023).

4.2. Cloud Computing als Auftragsdatenbearbeitung

Cloud Computing stellt eine Auftragsdatenbearbeitung dar. Diese birgt aber grössere Risiken in sich als andere Auslagerungen. Zu den zusätzlichen Risiken, die sich bei der Auslagerung in die Cloud für den Datenschutz ergeben, gehört ungenügende Transparenz über die Bearbeitung von Personendaten durch die Cloud-Anbieterin – einschliesslich der Daten von Angestellten des öffentlichen Organs zur Nutzung der Cloud-Anwendung – womit unter anderem die Einhaltung der Zweckbindung nicht richtig eingeschätzt werden kann. Weitere Risiken sind erschwerte Kontrollmöglichkeiten für die Auftraggeberin und für die Aufsichtsbehörde, der Einfluss ausländischer Rechtsordnungen und die Gewährleistung eines gleichwertigen Datenschutzes, die Portabilität der Daten und die Interoperabilität mit anderen Systemen sowie Datenverlust und Datenmissbrauch. Schliesslich hat der Auftraggeber kaum oder keine Einflussmöglichkeiten auf die Ausgestaltung der Cloud-Lösung. Er sieht sich oft vor der Entscheidung, das Angebot wie angeboten anzunehmen oder ganz darauf zu verzichten. Besondere Anliegen können oft nicht berücksichtigt werden.[34]

Es ist bei der Entscheidung und Umsetzung der Cloud-Lösung analog der Auftragsdatenbearbeitung vorzugehen. Die besonderen Risiken sind dabei einzubeziehen. Wichtigster Punkt dabei ist, dass der Auftraggeber für die Datenbearbeitung vollumfänglich verantwortlich bleibt, auch wenn das Bearbeiten im Ausland stattfindet, wie dies bei der Inanspruchnahme von Cloud-Lösungen häufig der Fall ist.[35]

4.3. Anwendbares Datenschutzrecht

Das Datenschutzrecht ist in der Schweiz in einem Bundesgesetz und in 26 kantonalen Gesetzen geregelt. Diese Regelung auf unterschiedlichen staatlichen Ebenen ergibt sich aus der Kompetenzordnung zwischen den drei staatlichen Ebenen (Bund, Kanton, Gemeinden) und führt zu einem föderalistisch geprägten Datenschutzsystem[36]. Der Bund hat die verfassungsmässige Kompetenz, Regelungen für die Bundesorgane (Art. 164 Abs. 1 lit. g BV, Art. 173 Abs. 2 BV) sowie für Private (betreffend Datenschutz: Privatwirtschaftliche Erwerbstätigkeit (Art. 95 Abs. 1 BV), Schutz der Konsumentinnen und Konsumenten (Art. 97 Abs. 1 BV), Zivilrecht (Art. 122 Abs. 1 BV), Strafrecht (Art. 123 Abs. 1 BV)) zu erlassen. Die Kantone haben aufgrund ihrer verfassungsrechtlich garantierten Organisationsautonomie (Art. 3, 46, 47 und 51 BV) die Kompetenz, für kantonale öffentliche Institutionen Regelungen zu erlassen. Entsprechend unterscheiden sich die Gesetze insbesondere betreffend Anwendungsberei-

---

[34] BRUNO BAERISWYL, Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht, in: digma 2019, S. 120; PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, V 3.0 / 03.02.2022, S. 2 ff., abrufbar unter: <https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf> (zuletzt besucht am 29.04.2023).

[35] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Merkblatt Cloud Computing, V 1.6 / Juli 2022, S. 1 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf> (zuletzt besucht am 29.04.2023).

[36] EVA MARIA BELSER, § 5 Die Kompetenzverteilung zwischen Bund und Kantonen, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Stämpfli 2011, Rn. 6.

che. Das Bundesgesetz ist für Bundesorgane sowie für private Datenbearbeiter anwendbar, die kantonalen Datenschutzgesetze kommen für die kantonalen öffentlichen Institutionen zur Anwendung. Dabei gelten diese Gesetze neben einander und sind nicht von einander abhängig, d.h. insbesondere, dass das Bundesgesetz den kantonalen Gesetzen keine Vorgaben macht und diese nicht beeinflusst. Die Regelungen haben sich einzig an den Vorgaben des Grundrechts auf informationelle Selbstbestimmung sowie der verfassungsmässigen Prinzipien der Bundesverfassung auszurichten. Inhaltlich unterscheiden sich daher die Gesetze nicht gross.[37]

Eine Institution, die eine Datenbearbeitung auslagern möchte, hat sich als ersten Schritt also die Frage zu stellen, welches Datenschutzrecht auf sie anwendbar ist. Für Bundesorgane ist es das DSG des Bundes (wie für private Datenbearbeitende auch), für kantonale Organe ist es das jeweilige kantonale Datenschutzgesetz.

Im Folgenden wird grundsätzlich beispielhaft anhand des Gesetzes über die Information und den Datenschutz des Kantons Zürich[38] vorgegangen.

4.4. Rechtliche Grundlagen für die Auftragsdatenbearbeitung

Öffentliche Institutionen sind in der Entscheidung, eine Auftragnehmerin für eine Aufgabenerfüllung beizuziehen, frei. Da bei der Auftragsdatenbearbeitung aber höhere Risiken für die Grundrechte der betroffenen Personen bestehen, werden die Rahmenbedingungen für den Beizug einer dritten Person in den Datenschutzgesetzen präzisiert. Insgesamt dürfen mit der Auslagerung einer Datenbearbeitung die betroffenen Personen in ihren Rechten nicht schlechter gestellt werden.[39]

Die Datenschutzgesetze sehen jeweils ähnliche Bestimmungen zur Auftragsdatenbearbeitung vor. Beispielhaft sei das Datenschutzgesetz des Bundes sowie jenes des Kantons Zürich aufgeführt.

Das revidierte neue Bundesgesetz über den Datenschutz (nDSG, SR 235.1)[40], das am 1. September 2023 in Kraft tritt, hält zur Auftragsdatenbearbeitung fest:

> ***Art. 9 Bearbeitung durch Auftragsbearbeiter***
>
> *1 Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:*
>
> *a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und*
>
> *b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.*

[37] Zum Ganzen: DOMINIKA BLONSKI, Was bedeutet die Revision für die kantonalen Datenschutzgesetze?, in: Astrid Epiney/Sophie Moser/Sophia Rovelli (Hrsg.), Die Revision des Datenschutzgesetzes des Bundes. La révision de la Loi fédérale sur la protection des données, Tagungsband zum Vierzehnten Schweizerischen Datenschutzrechtstag, 10. September 2021, Universität Fribourg, Schulthess 2022, S. 89 ff.

[38] Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG), LS 170.4.

[39] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 4.

[40] Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG), SR 235.1.

2 Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

4 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Im Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG, LS 170.4) ist die Auftragsdatenbearbeitung wie folgt umschrieben:

§ 6 Bearbeiten im Auftrag

1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.

2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.

4.5. Voraussetzungen für die Auftragsdatenbearbeitung

Aus den erwähnten Bestimmungen ergibt sich kumulativ, dass eine Auslagerung und damit Auftragsdatenbearbeitung grundsätzlich zulässig ist, wenn folgende Bedingungen und Voraussetzungen eingehalten sind:

- Es liegt keine rechtliche Bestimmung (wie Geheimhaltungsvorschriften) oder vertragliche Vereinbarung vor, die der Auslagerung entgegensteht.
- Der Auftraggeber nimmt seine Verantwortung wahr. Dies bedeutet, dass er (in der Regel vertraglich) sicherstellen muss, dass die Auftragnehmerin die Daten nur so bearbeitet, wie er selbst es tun dürfte. Zudem muss er sich vergewissern, dass die Auftragnehmerin die Datensicherheit gewährleisten kann.

4.5.1. Keine entgegenstehende rechtliche oder vertragliche Bestimmung

Bei der Auslagerung einer Auftragsdatenbearbeitung darf keine rechtliche oder vertragliche Bestimmung entgegenstehen. Damit ist klar, dass grundsätzlich ausgelagert werden darf, es sei denn, eine rechtliche oder vertragliche Bestimmung steht entgegen.[41]

Soweit bei der Auslagerung eine technische Lösung eingesetzt wird, die verhindert, dass die Cloud-Anbieterin von den Informationen und Personendaten Kenntnis erlangen kann, sind die Geheimhaltungsvorgaben bei der Auslagerung unbeachtlich. Technische Lösungen, die hier in Betracht gezogen werden, sind die Verschlüsselung, wobei die Cloud-Anbieterin über keinen Schlüssel zu den Daten verfügen darf, die Anonymisierung oder die Pseudonymisierung (mit Entschlüsselungsschlüssel beim Auftraggeber).[42]

---

[41] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 5.

[42] WOLFGANG WOHLERS, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015, S. 20; BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 3.

Als entgegenstehende rechtliche Bestimmung kommen insbesondere Geheimhaltungspflichten in Frage. So kann ein Amtsgeheimnis, ein besonderes Amtsgeheimnis (wie das Steuergeheimnis oder das Sozialhilfegeheimnis) oder ein Berufsgeheimnis der Auslagerung entgegenstehen.[43] Solche Geheimhaltungsverpflichtungen sind in zahlreichen Gesetzen festgehalten. So sieht beispielsweise das Personalgesetz des Kantons Zürich eine Schweigepflicht für Mitarbeitende des Kantons Zürich vor.[44] Auch das Gesundheitsgesetz des Kantons Zürich sieht eine Schweigepflicht für Mitarbeitende im Gesundheitswesen vor.[45] Diese Geheimhaltungspflichten sind zudem strafbewehrt gemäss Strafgesetzbuch.[46]

Ob eine solche Geheimhaltungsverpflichtung der Auslagerung entgegensteht, muss durch Auslegung der Bestimmung, die die Geheimhaltungsverpflichtung umschreibt, im Einzelfall eruiert werden.

Amtsgeheimnis

Das Amtsgeheimnis schützt das Amt insbesondere in seiner Funktionstüchtigkeit. Dem Geheimnis steht das Öffentlichkeitsprinzip gegenüber. Dieses bewirkt, dass Informationen öffentlich sind, wenn nicht ein Geheimhaltungsinteresse entgegensteht. Damit kann und muss das Amt selber entscheiden, welche Informationen der Schweigepflicht unterliegen müssen, damit die Funktionstüchtigkeit gewährleistet ist und somit ein Geheimhaltungsinteresse besteht. Folglich können Informationen, die dem Amtsgeheimnis unterliegen grundsätzlich in die Cloud ausgelagert werden. Die Mitarbeitenden der Cloud-Anbieterin sind vertraglich in die Geheimnispflicht einzubinden. Sie werden aus strafrechtlicher Perspektive zu Hilfspersonen des Geheimnisträgers und der Auftraggeber selber ist in diesem Fall nicht strafbar. Werden sie nicht in die Geheimnispflicht eingebunden, machen sich die Mitarbeitenden der öffentlichen Institution, die dem Geheimnis untersteht, strafbar, wobei dafür bereits der Versuch genügt, d.h. die Möglichkeit der Kenntnisnahme ist für die Bejahung der Strafbarkeit ausreichend.[47]

Besondere Amtsgeheimnisse

Die besonderen Amtsgeheimnisse – wie beispielsweise das Steuergeheimnis oder das Sozialhilfegeheimnis – vereinen neben dem Amtsgeheimnis, das die Funktionstüchtigkeit des Amtes schützt, auch die Sicherstellung des Vertrauensverhältnisses zwischen dem Staat und den Bürgerinnen und Bürgern. Damit gewähren sie auch den Schutz der Grundrechte und der Persönlichkeit der betroffenen Personen, deren Personendaten bearbeitet werden. Im Unterschied zum gewöhnlichen Amtsgeheimnis gelten die besonderen Amtsgeheimnisse daher absolut und stehen der Offenbarung entgegen, soweit keine rechtliche Grundlage die Weitergabe der

---

[43] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 5, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

[44] § 51 Personalgesetz des Kantons Zürich vom 27. September 1998 (PG), LS 177.10.

[45] § 15 Gesundheitsgesetz des Kantons Zürich vom 2. April 2007 (GesG), LS 810.1.

[46] Art. 320 und 321 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

[47] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 41 ff.

Informationen vorsieht. Bei den besonderen Amtsgeheimnissen stellt sich die Frage, ob die Cloud-Anbieterin die erhöhten Anforderungen an die Geheimhaltung einhalten kann. Dies ist insbesondere bei Cloud-Anbietern im Ausland oder bei solchem mit einem US-Bezug nicht der Fall.[48]

Berufsgeheimnis

Beim Berufsgeheimnis ist der Geheimnisherr die betroffene Person. Damit kann nicht der Geheimnisträger darüber entscheiden, welche Informationen dem Geheimnis unterliegen – die Geheimnispflicht gilt absolut. Informationen und Daten dürfen deshalb nur vom Berufsgeheimnisträger oder dessen Hilfspersonen bearbeitet werden, ausser eine gesetzliche Grundlage bestimmt etwas anderes, oder es liegt die Einwilligung der betroffenen Person im Einzelfall oder eine Aufhebung des Berufsgeheimnisses durch die vorgesetzte Behörde im Einzelfall vor. Die Auslagerung in die Cloud hängt deshalb davon ab, ob die Mitarbeitenden der Cloud-Anbieterin als Hilfspersonen qualifiziert werden können. Dies ist nur der Fall, wenn ein direktes Weisungsrecht besteht, was bei internationalen Cloud-Anbieterinnen mit Standardlösungen regelmässig nicht der Fall ist, weshalb öffentliche Institutionen Informationen und Daten unter dem Berufsgeheimnis ohne technische Massnahmen, die eine Kenntnisnahme verhindern, nicht auslagern können. Eine vertragliche Einbindung in das Geheimnis ist beim Berufsgeheimnis nicht möglich. Auch eine Einwilligung fällt in diesem Kontext – anders als bei privaten Datenbearbeitenden – weg. Denn dort kann die betroffene Person einwilligen, womit die Auftragnehmerin bei Vorliegen eines Berufsgeheimnisses zur Hilfsperson wird. Das Berufsgeheimnis steht damit einer Auslagerung in die Cloud durch eine öffentliche Institution entgegen.[49]

Vertragliche Vereinbarungen

Des Weiteren können vertragliche Vereinbarungen der Auslagerung entgegenstehen. So kann beispielsweise der Datenbearbeiter mit der betroffenen Person vertraglich eine Geheimhaltung vereinbaren. Diese Vereinbarung lässt sich in der Regel auf die Auftragnehmerin überbinden. Oder die weitere Auslagerung an Unterauftragnehmende wird vertraglich ausgeschlossen, so dass diese nicht zulässig ist bzw. zu einer Verletzung der Vereinbarung führt.[50]

Klassifizierungen

Schliesslich können Klassifizierungen von Informationen zu Geheimhaltungsverpflichtungen führen. So sieht beispielsweise das neue Informationssicherheitsgesetz des Bundes[51] vor, dass bestimmte Informationen nicht zugänglich gemacht werden dürfen. Dies ist beispielsweise der

---

[48] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 46 f.

[49] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 50 ff.

[50] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 35 f.

[51] Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz, ISG), SR 128.

Fall, wenn dies die Interessen der inneren und/oder äusseren Sicherheit der Schweiz schwerwiegend beinträchtigen könnte.[52]

Weitere entgegenstehende Bestimmungen

Schliesslich können weitere Bestimmungen einer Auslagerung entgegenstehen bzw. diese einschränken. So sieht beispielsweise die Verordnung über das elektronische Patientendossier[53] vor, dass sich die Datenspeicher, auf denen die Informationen des Patientendossiers abgelegt werden, in der Schweiz befinden müssen und dem Schweizer Recht zu unterstehen haben (Art. 12 Abs. 5 EPDV).

4.5.2. Wahrnehmung der Verantwortung

Der Auftraggeber bleibt bei der Auslagerung verantwortlich für die Datenbearbeitung. Er nimmt seine Verantwortung zunächst bei der Auswahl der Auftragnehmerin, später deren Instruktion sowie Überwachung wahr. Er muss zudem die Einhaltung des Datenschutzes auch gewährleisten, wenn die Datenbearbeitung ausgelagert wird. Dies umfasst die Sicherstellung, dass die Auftragnehmerin die Daten nur so bearbeitet, wie dies der Auftraggeber selbst auch tun dürfte. Das wird in der Regel im Rahmen eines schriftlichen Vertrages sichergestellt. Schliesslich hat sich der Auftraggeber zu vergewissern, dass die Auftragnehmerin die Datensicherheit gewährleisten kann und dies auch tut.

Auswahl der Auftragnehmerin

Der Auftraggeber hat die in Auftragsverhältnissen übliche Sorgfaltspflicht auszuüben und haftet entsprechend für Schäden, die die Auftragnehmerin verursacht (Art. 55 OR[54]). Daher hat er die Auftraggeberin sorgfältig auszuwählen, zu instruieren und bei der Aufgabenerfüllung zu überwachen. Die Auftragnehmerin untersteht dem Weisungsrecht des Auftraggebers. Eine Auslagerung ist nur möglich, wenn dieses Weisungsrecht bei der jeweiligen Auftragnehmerin durchgesetzt werden kann. Zudem hat der Auftraggeber zu prüfen, ob die Auftragnehmerin seine Vorgaben überhaupt einhalten kann. Ist dies nicht der Fall, darf die Auftragnehmerin nicht für die Auftragsdatenbearbeitung ausgewählt werden.[55]

Diese Sorgfaltspflicht bei der Auswahl erstreckt sich zunächst auf die potentielle Auftragnehmerin selber. Der Auftraggeber hat also zu prüfen, wie diese aufgestellt ist und wie sie arbeitet. Sodann hat er ihr (Rechts-)Umfeld zu evaluieren. Es stellt sich dabei die Frage, ob der Auftrag überhaupt in einem für den Auftraggeber vertretbaren juristischen Umfeld erfolgen kann. Ist dies nicht der Fall, scheidet die Auftraggeberin bereits bei der Auswahl aus,

---

[52] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 38.

[53] Verordnung über das elektronische Patientendossier vom 22. März 2017 (EPDV), SR 816.11.

[54] Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (OR), SR 220.

[55] VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 16; BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 2.

denn der öffentlich-rechtliche Auftraggeber hat sich an seine gesetzlichen Vorgaben zu halten und kann nichts auf die betroffenen Personen abwälzen (wie dies im Gegensatz dazu in einer privat-rechtlichen Konstellation mittels AGB, Einwilligung usw. möglich wäre).

Schriftlicher Vertrag

Der Auftraggeber muss die Einhaltung des Datenschutzes gewährleisten und sicherstellen, dass die Auftragnehmerin die Daten nur so bearbeitet, wie dies der Auftraggeber selbst auch tun dürfte.[56]

Dafür schliesst er zunächst mit der Auftragnehmerin einen Vertrag ab, der die wesentlichen Punkte regelt. Der Regierungsrat des Kantons Zürich erliess dafür beispielsweise die AGB Auslagerung Informatikleistungen[57] und die AGB Datenbearbeitung durch Dritte[58]. Die öffentlichen Organe der kantonalen Verwaltung müssen diese AGB in ihre Verträge mit Cloud-Anbieterinnen einbeziehen. Sie regeln zentrale Punkte zur Verantwortung für die Datenbearbeitung wie die Zweckbindung, den Umgang mit Unterauftragnehmenden, das anwendbare Recht, den Gerichtsstand, bestimmte Massnahmen zur Informationssicherheit und die Kontrollmöglichkeiten. Liegen keine solche AGB vor, sind folgende Punkte vertraglich mit der Auftragnehmerin zu vereinbaren:[59]

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (muss beim öffentlichen Organ liegen)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen
- Geheimhaltungsverpflichtungen
- Rechte Betroffener (Auskunft)
- Informationssicherheitsmassnahmen
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung oder mindestens einer Information auf der Website oder per E-Mail oder anderweitige Ankündigung mit möglicher Vertragsbeendigung)
- Entwicklung und Wartung

---

[56] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 30.

[57] Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen des Kantons Zürich (AGB Auslagerung Informatikleistungen) vom 24. Juni 2015, abrufbar unter: <https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_auslagerung_informatikleistungen.pdf> (zuletzt besucht am 29.04.2023).

[58] Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte des Kantons Zürich (AGB Datenbearbeitung durch Dritte) vom 24. Juni 2015, abrufbar unter: <https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_datenbearbeitung_durch_dritte.pdf> (zuletzt besucht am 29.04.2023).

[59] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 8 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

- Orte der Datenbearbeitung (Schweiz oder bei Bearbeiten im Ausland gleichwertiges Datenschutzniveau oder zusätzliche Massnahmen)
- Cloud Computing (den zusätzlichen Risiken angepasste Massnahmen)
- Geschäftsgeheimnis
- Werbung
- Sanktionen
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Löschung nach Vertragsauflösung
- Datenportabilität
- Haftung
- Verhältnis zu anderen geltenden AGB
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand)

Auf einen wichtigen vertraglich zu regelnden Punkt soll besonders hingewiesen werden. Die Auftragnehmerin darf die Daten nicht zu ihren eigenen Zwecken bearbeiten. Für eine rechtskonforme eigene Datenbearbeitung muss eine Rechtsgrundlage für eine Datenbekanntgabe vorliegen. Dies kann nicht beispielsweise mit AGBs der Cloud-Anbieterin ausbedungen werden. Vielmehr ist eine solche Verwendung zu eigenen Zwecken strafbewehrt (§ 40 IDG).[60]

Datensicherheit – Organisatorisch-Technische Massnahmen

Der Auftraggeber muss – wie bei der Datenbearbeitung durch ihn – auch bei der Auslagerung angemessene organisatorische und technische Massnahmen treffen. Lagert er die Datenbearbeitung aus, hat er sich zu vergewissern, dass die Auftragnehmerin die Datensicherheit gewährleisten kann und dies auch tut. Das heisst, er muss angemessene organisatorische und technische Massnahmen von der Cloud-Anbieterin einfordern und überprüfen, ob diese die Massnahmen umsetzen kann.[61]

Die Festlegung der erforderlichen Massnahmen, die angemessen sein müssen, erfolgt gestützt auf eine Risikobeurteilung. Als Massnahme zur Minderung der Risiken spielt die Verschlüsselung eine grosse Rolle. Werden Personendaten (unter anderem) in Datenzentren in Ländern ohne gleichwertiges Datenschutzniveau bearbeitet oder gespeichert, müssen sie verschlüsselt werden und der Schlüssel muss beim öffentlichen Organ liegen. Werden die Daten in Datenzentren im Inland oder in einem Land mit gleichwertigem Datenschutzniveau bearbeitet, sind einzig die besonderen Personendaten zu verschlüsseln und der Schlüssel muss nur dann beim öffentlichen Organ liegen, wenn dies eine Beurteilung der Risiken ergibt. Sollte der Verbleib des Schlüssels beim öffentlichen Organ nicht möglich sein, kann alternativ eine vertragliche Abmachung getroffen werden, wonach die Cloud-Anbieterin den Schlüssel nur auf explizite

[60] BRUNO BAERISWYL, Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht, in: digma 2019, S. 119.

[61] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 55 ff.

Anfrage und nach expliziter Einwilligung des öffentlichen Organs einsetzen und auf die Daten zugreifen darf.[62]

4.6. Methodisches Vorgehen

Bei der Abklärung der Frage, ob eine Datenbearbeitung in die Cloud ausgelagert werden kann, ist ein methodisches Vorgehen zu wählen. Die Projektmethode HERMES ist dafür in der Schweiz bei öffentlichen Institutionen weit verbreitet, im Kanton Zürich[63] ist sie für die kantonale Verwaltung verbindlich vorgeschrieben. Die Methode gewährleistet in einem schrittweisen Vorgehen, dass die datenschutzrechtlichen Vorgaben richtig berücksichtigt werden. Sie sieht eine Rechtsgrundlagenanalyse, eine Schutzbedarfs- und Risikoanalyse und die Erstellung eines Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) vor. Zudem wird eine Datenschutz-Folgenabschätzung (DSFA) und allenfalls eine Vorabkontrolle bei der Datenschutzbeauftragten durchgeführt.

Ist die HERMES-Methode nicht verpflichtend vorgegeben, kann dennoch analog vorgegangen werden. Denn die Schritte ergeben sich auch unabhängig der gewählten Methodik aus dem jeweiligen Gesetz. So sehen sowohl das neue Datenschutzgesetz des Bundes als auch die gestützt auf den Schengen-Nachvollzug im Polizei- und Justizbereich in den letzten Jahren revidierten kantonalen Datenschutzgesetze bei einer geplanten Datenbearbeitung neu immer eine Datenschutz-Folgenabschätzung (DSFA) und eine Vorabkontrolle bei der Datenschutzbeauftragten vor.

Rechtsgrundlagenanalyse

In der Rechtsgrundlagenanalyse[64] ist unter anderem zu beurteilen, wie weit Geheimhaltungsverpflichtungen oder Zugriffsmöglichkeiten von ausländischen Behörden (z.B. CLOUD Act) einer Auslagerung entgegenstehen. Dabei geht es um die Auslegung der einschlägigen Gesetzesbestimmungen (Amtsgeheimnis, besondere Amtsgeheimnisse und Berufsgeheimnis) sowie um die Frage, ob der Zugriff von ausländischen Behörden im Rahmen der ordentlichen Rechtshilfe erfolgt oder dem schweizerischen ordre public widerspricht und somit rechtswidrig ist und durch technische Massnahmen wie Verschlüsselung zu unterbinden ist oder allenfalls auf die Auslagerung zu verzichten ist.

Schutzbedarfs- und Risikoanalyse

Nach der Rechtsgrundlagenanalyse folgt die Schutzbedarfsanalyse[65] oder auch Risikoanalyse genannt. Nachdem in der Rechtsgrundlagenanalyse festgestellt wurde, welche Informationen

---

[62] DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung – unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten, V 2.3 / Juli 2022, S. 1, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

[63] Regierungsratsbeschluss des Kantons Zürich Nr. 903 vom 27. September 2017 (RRB 903/2017).

[64] Die HERMES-Vorlage für eine Rechtsgrundlagenanalyse ist abrufbar unter: <https://hermes.zh.ch/anwenderloesung/vorlagen.xhtml> (zuletzt besucht am 29.04.2023).

[65] Die HERMES-Vorlage für eine Schutzbedarfsanalyse ist abrufbar unter: <https://hermes.zh.ch/anwenderloesung/vorlagen.xhtml> (zuletzt besucht am 29.04.2023).

und Daten rechtmässig in der Cloud bearbeitet werden können, ist festzulegen, mit welchen technischen und organisatorischen Massnahmen die verbleibenden Risiken zu minimieren sind. Dabei sind dem Risiko angemessene Massnahmen zum Schutz der Informationen und Daten zu treffen.

ISDS-Konzept

Ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)[66] fasst die Ausführungen der Schutzbedarfsanalyse zusammen und bildet die Ausgangslage für die Umsetzung des Projekts.

Datenschutz-Folgenabschätzung (DSFA)

Die Rechtsgrundlagenanalyse, die Schutzbedarfs- und Risikoanalyse und das ISDS-Konzept sind auch die Grundlage für die bei einer beabsichtigten Datenbearbeitung erforderliche Datenschutz-Folgenabschätzung (DSFA)[67]. Darin müssen die Risiken des Projekts für die Grundrechte der betroffenen Personen aufgezeigt werden. Gleichzeitig sind angemessene organisatorische und technische Massnahmen zu beschreiben, welche die Risiken reduzieren. Ohne DSFA können die öffentlichen Institutionen die konkreten Risiken des Cloud-Projekts weder identifizieren noch angemessen mit ihnen umgehen.

Vorabkontrolle

Ergibt sich aus der DSFA, dass besondere Risiken für die Grundrechte der betroffenen Personen vorliegen, muss das Projekt vorab der Datenschutzbeauftragten zur Vorabkontrolle unterbreitet werden.[68] Dies dürfte bei der Auslagerung in die Cloud (wie beispielsweise mit der Einführung von Microsoft 365) regelmässig der Fall sein. Eingereicht werden muss die Beschreibung des Projekts, die Darstellung der Rechtslage und eine Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen. Dazu gehört insbesondere die DSFA und das ISDS-Konzept zur Einführung einer Cloud-Lösung.

4.7. Auslagerungen mit Auslandbezug

Immer mehr werden Aufgaben und damit auch Datenbearbeitungen nicht nur in der Schweiz an schweizerische Unternehmen oder Institutionen ausgelagert, sondern auch öffentliche Institutionen ziehen vermehrt ausländische Anbieterinnen bei oder übertragen die Datenbearbeitung gar ins Ausland. Auf die Besonderheiten dieser beiden Szenarien gehen die nächsten Abschnitte ein.

---

66 Die HERMES-Vorlage für ein ISDS-Konzept ist abrufbar unter: <https://hermes.zh.ch/anwenderloesung/vorlagen.xhtml> (zuletzt besucht am 29.04.2023).

67 Die Datenschutzbeauftragte stellt eine Vorlage für eine DSFA zur Verfügung, abrufbar unter: <https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung> (zuletzt besucht am 29.04.2023).

68 Weitere Informationen zur Vorabkontrolle stellt die Datenschutzbeauftragte zur Verfügung, abrufbar unter: <https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung#wann-besteht-die-pflicht-zur-vorabkontrolle-0904a5f2-5db8-4d7a-bbb8-2e27b4a44cb7> (zuletzt besucht am 29.04.2023).

4.7.1. Auslagerung ins Ausland

Mit der Übermittlung von Personendaten ins Ausland im Rahmen der Auslagerung, steigen die Risiken für die Grundrechte der betroffenen Personen. Gleichzeitig steigen auch die Risiken für den Auftraggeber. Denn die sich im Ausland befindenden Daten sind einer Rechtsordnung ausgesetzt, die dem Auftraggeber fremd ist und deren Auswirkungen er nicht einschätzen kann. Es kann zum Beispiel die Weitergabe der Daten vorgesehen sein. Diese Risiken erschweren Kontrollen durch den Auftraggeber. Folglich muss er weitere Massnahmen ergreifen.[69]

Welche Massnahmen ergriffen werden müssen, hängt von der Art der Daten ab und auch davon, ob das Datenschutzniveau im konkreten Land dem schweizerischen Datenschutz angemessen ist. Die Gesetze halten fest, dass dies der Fall ist, wenn die Konvention 108[70] anwendbar ist bzw. das jeweilige Land dieser Konvention beigetreten ist (§ 19 IDG i.V.m. § 22 IDV[71]). In diesem Fall müssen keine zusätzlichen Massnahmen ergriffen werden.[72]

4.7.2. Auslagerung bei Anwendbarkeit des CLOUD Act

Etwas komplexer wird die Konstellation, wenn der CLOUD Act[73] bei einer Auslagerung zur Anwendung kommt. Der CLOUD Act ist ein Gesetz der USA, das es bestimmten US-Behörden ermöglicht, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Es handelt sich dabei somit um ein Gesetz mit extraterritorialer Wirkung. Dieses Verfahren und dieser Zugriff auf Daten ist mit dem Datenschutzrecht und dem übergeordneten schweizerischen Recht nicht vereinbar. Es verstösst gegen den ordre public der Schweiz, weil es eine Umgehung des internationalen Rechtshilfewegs darstellt.[74]

Soll an ein US-amerikanisches Unternehmen, das aufgrund dieser Eigenschaft dem CLOUD Act untersteht, ausgelagert werden, muss folglich eine technische Lösung die unrechtmässige Kenntnisnahme unter dem CLOUD Act verhindern. Ist dies der Fall, kann ohne Weiteres ausgelagert werden. In Frage kommen die Verschlüsselung mit Schlüsselmanagement bei der öffentlichen Institution, die Anonymisierung oder die Pseudonymisierung der Daten, wobei auch hier die Re-Identifikationsmerkmale bei der öffentlichen Institution verbleiben müssen.

Neben diesem Grundsatz ist auch beim CLOUD Act zwischen den verschiedenen Geheimhaltungsverpflichtungen zu unterscheiden. Das Berufsgeheimnis schliesst eine Auslagerung aus,

---

69 VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 27 f.

70 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108), SR 0.235.1.

71 Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV), LS 170.41.

72 VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 27; BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 65 ff.

73 Clarifying Lawful Overseas Use of Data Act, abrufbar unter: <https://www.congress.gov/bill/115th-congress/senate-bill/2383> (zuletzt besucht am 29.04.2023).

74 BUNDESAMT FÜR JUSTIZ, Bericht zum US CLOUD Act, 17. September 2021, S. 35.

wenn nicht technische Massnahmen ergriffen werden, die die Kenntnisnahme durch die Auftragnehmerin verhindern. Analoges gilt für besondere Amtsgeheimnisse. Beim gewöhnlichen Amtsgeheimnis ist zunächst durch die öffentliche Institution zu entscheiden, ob eine Information dem Amtsgeheimnis untersteht.[75]

In einem nächsten Schritt müssen die angemessenen Massnahmen passend zur Art der Personendaten ergriffen werden. Bei normalen Personendaten können unterschiedliche Massnahmen ausreichend sein. Für besondere Personendaten kommt die Risikoabwägung zum Schluss, dass eine Kenntnisnahme unterbunden werden muss. Das heisst, es ist eine Verschlüsselung zu implementieren, deren Schlüsselmanagement bei der öffentlichen Institution verbleibt.

Vereinzelt wird die Meinung vertreten, es könne der rechtlichen Frage, ob eine Auslagerung zulässig ist – i.S.v. dass keine Bestimmungen entgegenstehen –, anhand einer Risikoabwägung mit Wahrscheinlichkeitsberechnungen begegnet werden. Es führt nicht weiter, diese Rechtsfrage mit dem Argument zu umgehen, die Wahrscheinlichkeit eines solchen rechtswidrigen Zugriffs unter dem CLOUD Act sei klein. Einerseits wird verkannt, dass ein öffentliches Organ das Recht immer zu beachten und sich rechtmässig zu verhalten hat («Legalitätsprinzip»), und andererseits kann das Verhalten einer amerikanischen Strafbehörde mit einer Methode mit Wahrscheinlichkeitsberechnungen nicht vorausgesagt werden. Der CLOUD Act verstösst gegen den ordre public, weil das vorgesehene Verfahren unter dem CLOUD Act (auch internationale) verfahrensrechtlichen Prinzipien aushebelt, indem beispielsweise keine Rechte Betroffener vorgesehen sind. Für den Anbieter ergibt sich damit das Problem, dass er dem Auftraggeber nicht garantieren kann, sich nach internationalem Recht zu verhalten. Entsprechend hat das der Auftraggeber bei der Auswahl der Auftragnehmerin zu beachten, wobei er sich hier nicht auf Wahrscheinlichkeiten stützen kann. Recht ist einzuhalten.[76]

Daraus ergibt sich, dass bei Geheimnispflichten, die entgegenstehen (besondere Amtsgeheimnisse und Berufsgeheimnis als rechtliche entgegenstehende Bestimmungen), nicht ohne Schutz, der die Offenbarung dieser Geheimnisse verhindert (d.h. Verschlüsselung so, dass Schlüssel für Anbieter nicht zugänglich, also bei der öffentlichen Institution), an einen Anbieter ausgelagert werden kann, der dem CLOUD Act untersteht. Denn dieser kann – unabhängig der Wahrscheinlichkeit eines Zugriffs – nicht garantieren, dass der übliche Rechtsweg (und damit internationales Recht, inkl. Betroffenenrechte usw., also der ordre public) eingehalten wird. Die öffentliche Institution kommt also schon bei der Auswahl des Anbieters zum Schluss, dass die Geheimnispflichten entgegenstehen. Dies kann nicht durch tiefe Wahrscheinlichkeiten geheilt werden.

Das betrifft die besonderen Amtsgeheimnisse und das Berufsgeheimnis, weil hier das Amt nicht oder nicht alleine Geheimnisherr ist. D.h. es kann nicht selber über den Geheimhaltungswillen entscheiden. Beim normalen Amtsgeheimnis kann es hingegen selber entschei-

---

[75] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 71 f.

[76] BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 76.

den, was es dem Amtsgeheimnis unterstellen möchte und entsprechend die Auftragnehmerin in das Geheimnis einbinden. Daher kann es hier bei der Festlegung von «angemessenen» Massnahmen zum Schutz entscheiden, welche Art von Verschlüsselung angemessen ist, das kann beispielsweise bei normalen Personendaten auch ein Lockbox-Prozess sein, bei besonderen Personendaten bräuchte es mehr. Diese zweite Überlegung zu den «angemessenen» Massnahmen ergibt sich aber aus der Risikoabwägung und nicht aus der Frage, ob eine rechtliche Bestimmung entgegen steht.

5. Handlungsanleitung

Die Ausführungen dieser MAS-Arbeit können im Ergebnis wie folgt in einer tabellarischen Handlungsanleitung zusammengefasst und dargestellt werden. Die staatlichen Institutionen können anhand dieser Darstellung vorgehen und stellen sich so die richtigen Fragen im richtigen Moment.

Tabelle 1: Handlungsanleitung

Frage / Thema	Antwort / Inhalte	To Do	Methodik
Liegt eine **staatliche Aufgabe** vor?	Ja.	Nächste Frage.	
	Nein.	Ende	
Keep in Mind: Besondere Verantwortung gegenüber Bevölkerung, weil:	- Unter-/Überordnungsverhältnis (Machtgefälle) - keine Wahlmöglichkeit - keine Freiwilligkeit - Einhaltung verfassungsmässige Prinzipien, insbesondere: Grundrechte, Legalitätsprinzip		
Ist diese Aufgabe **auslagerungsfähig**?	Ja.	Nächste Frage.	
	Nein.	Ende	
Strategisches	- Ziel - Anspruchsgruppen - Ressourcen / Kompetenzen - Prozesse / Strukturen - Wertschöpfung / Gemeinwohlbeitrag	Strategische Überlegungen / Analyse	
Werden **Personendaten** bearbeitet?	Ja.	Nächste Frage.	
	Nein.	Ende	
Welche **Art** von Personendaten wird bearbeitet?	«gewöhnliche» Personendaten	Angemessene Massnahmen nicht hoch.	
	Besonders schützenswerte Personendaten	Angemessene Massnahmen hoch.	
Welches **Datenschutzrecht** ist anwendbar?	DSG, IDG usw.	Nächste Frage.	

Frage / Thema	Antwort / Inhalte	To Do	Methodik
Kann die **Kenntnisnahme** der Personendaten **ausgeschlossen** werden?	Ja, mittels: - Verschlüsselung mit Schlüsselmanagement beim Auftraggeber - Anonymisierung - Pseudonymisierung	Ende	
	Nein.	Nächste Frage.	
Liegt eine rechtliche **Bestimmung** vor, die der Auslagerung **entgegensteht**?	Amtsgeheimnis	Nächste Frage.	Rechtsgrundlagenanalyse
	Besonderes Amtsgeheimnis	Falls CLOUD Act anwendbar oder keine Hilfspersoneneigenschaft: Ende oder Massnahmen, die Kenntnisnahme verhindern	
	Berufsgeheimnis		
	Vertragliche Vereinbarung	Ende oder Massnahmen, die Kenntnisnahme verhindern	
	Klassifizierung		
	weitere		
Ist der **CLOUD Act** anwendbar?	Ja.	Welche Geheimnispflicht liegt vor?	
	Nein.	Nächste Frage.	
Ausschreibung / **Beschaffung**	Definition der Anforderungen		
Auswahl der Auftragnehmerin: Kann sie Vorgaben erfüllen?	Ja.	Nächste Frage.	
	Nein.	Ende	
Kann ein rechtskonformer **Vertrag** abgeschlossen werden?	Ja.		
	Nein.		
Können **angemessene organisatorische und technische Massnahmen** ergriffen werden?	Ja.	Nächster Punkt.	Schutzbedarfs- und Risikoanalyse ISDS-Konzept
	Nein.	Ende	
Datenschutzbeauftragte			DSFA Vorabkontrolle

6. Vorgehensweise am Beispiel eines Spitals

Mit der erstellten Handlungsanleitung wird nun an einem konkreten Beispiel aufgezeigt, wie diese angewendet wird. Als Beispiel dient ein kantonales Spital im Kanton Zürich. Dieses möchte das Klinikinformationssystem in eine Cloud-Lösung eines amerikanischen Unternehmens auslagern.

Tabelle 2: Anwendung Handlungsanleitung auf Spital

Frage / Thema	**Antwort / Inhalte**	**To Do**	**Methodik**
Liegt eine **staatliche Aufgabe** vor?	Ja. *Spital ist öffentliche Institution.*	Nächste Frage.	
	Nein.	Ende	
Keep in Mind: Besondere Verantwortung gegenüber Bevölkerung, weil:	- Unter-/Überordnungsverhältnis (Machtgefälle) - keine Wahlmöglichkeit - keine Freiwilligkeit - Einhaltung verfassungsmässige Prinzipien, insbesondere: Grundrechte, Legalitätsprinzip		
Ist diese Aufgabe **auslagerungsfähig**?	Ja.	Nächste Frage.	
	Nein.	Ende	
Strategisches	- Ziel - Anspruchsgruppen - Ressourcen / Kompetenzen - Prozesse / Strukturen - Wertschöpfung / Gemeinwohlbeitrag	Strategische Überlegungen / Analyse	
Werden **Personendaten** bearbeitet?	Ja.	Nächste Frage.	
	Nein.	Ende	
Welche **Art** von Personendaten wird bearbeitet?	«gewöhnliche» Personendaten	Angemessene Massnahmen nicht hoch.	
	Besonders schützenswerte Personendaten *Gesundheitsdaten*	Angemessene Massnahmen hoch.	

Frage / Thema	Antwort / Inhalte	To Do	Methodik
Welches **Datenschutzrecht** ist anwendbar?	IDG	Nächste Frage.	
Kann die **Kenntnisnahme** der Personendaten **ausgeschlossen** werden?	Ja, mittels: - Verschlüsselung mit Schlüsselmanagement beim Auftraggeber - Anonymisierung - Pseudonymisierung	Ende	
	Nein.	Nächste Frage.	
Liegt eine rechtliche **Bestimmung** vor, die der Auslagerung **entgegensteht**?	Amtsgeheimnis	Nächste Frage.	Rechtsgrundlagenanalyse
	Besonderes Amtsgeheimnis	Falls CLOUD Act anwendbar oder keine Hilfspersoneneigenschaft: Ende oder Massnahmen, die Kenntnisnahme verhindern	
	Berufsgeheimnis		
	Vertragliche Vereinbarung	Ende oder Massnahmen, die Kenntnisnahme verhindern	
	Klassifizierung		
	weitere		
Ist der **CLOUD Act** anwendbar?	Ja.	Welche Geheimnispflicht liegt vor? *Berufsgeheimnis*	
	Nein.	Nächste Frage.	
Ausschreibung / **Beschaffung**	Definition der Anforderungen *Verschlüsselung mit Schlüsselmanagement beim Spital*		
Auswahl der Auftragnehmerin: Kann sie Vorgaben erfüllen?	Ja.	Nächste Frage.	
	Nein.	Ende	
Kann ein rechtskonformer **Vertrag** abgeschlossen werden?	Ja.		
	Nein.		

Frage / Thema	Antwort / Inhalte	To Do	Methodik
Können **angemessene organisatorische und technische Massnahmen** ergriffen werden?	Ja.	Nächster Punkt.	Schutzbedarfs- und Risikoanalyse ISDS-Konzept
	Nein.	Ende	
Datenschutzbeauftragte			DSFA Vorabkontrolle

7. Schlussfolgerungen und Zusammenfassung

Die MAS-Arbeit hat folgende Forschungsfrage untersucht:

> *Welche Aspekte sind durch öffentliche Institutionen zu berücksichtigen, wenn diese die Nutzung von neuen Technologien – am Beispiel von Cloud-Lösungen – in Erwägung ziehen?*

Um diese zu beantworten hat sie diese Frage aus fünf Perspektiven betrachtet: Staatstheoretische Perspektive, politische Perspektive, strategische Perspektive, juristische Perspektive und technische Perspektive. Bei der Auseinandersetzung mit den verschiedenen Perspektiven liessen sich die Rahmenbedingungen für eine Auslagerung in eine Cloud aufzeigen. Die Arbeit ist eine konzeptionelle Arbeit. Sie resultiert – gestützt auf die eruierten Rahmenbedingungen – in einer Handlungsanleitung.

Cloud Computing ist eine technische Lösung, die insbesondere Flexibilität und Skalierbarkeit mit sich bringt. Aber Cloud Computing birgt auch Risiken, die zu Kontroll- und Transparenzverlust führen. Die staatliche Institution muss sich die Frage stellen, ob und wie sie ihre Verantwortung wahrnehmen kann.

Der Staat hat gezielt zugeteilte Aufgaben. Er hat sich bei der Aufgabenerfüllung als Staat an die verfassungsmässigen Prinzipien zu halten. Besonders im Vordergrund stehen die Grundrechte der Bevölkerung, die eingehalten werden müssen, sowie das Legalitätsprinzip. Der Staat muss sich bewusst sein, dass sich seine Stellung von jener von privaten Akteuren unterscheidet, was dazu führt, dass er nicht gleich handeln kann. So besteht zwischen dem Staat und den Individuen ein Unter-/Überordnungsverhältnis, ein Machtgefälle. Die Individuen haben keine Wahlmöglichkeiten und es besteht keine Freiwilligkeit, sie können also – im Unterschied zu Rechtsverhältnissen unter Privaten – nicht einwilligen. Damit trägt der Staat eine besondere Verantwortung gegenüber den Individuen. Diese muss er auch im Rahmen der Auslagerung – nicht alle Aufgaben sind auslagerungsfähig, bei jenen, die es aber sind – wahrnehmen.

Hinzu kommt die Pflicht des Staates, Beschaffungen nach einem klar definierten Prozess vorzunehmen. Hierbei ist vorausgesetzt, dass der Staat die Anforderungen, die sich für ihn bei der Auslagerung – insbesondere auch wenn Cloud-Lösungen beigezogen werden – ergeben, in der Ausschreibung als Muss-Kriterien auflistet. Anbieterinnen, die diese Anforderungen nicht erfüllen können, kann der Zuschlag nicht erteilt werden.

Auch der Staat macht sich strategische Überlegungen, gerade, wenn er Cloud-Lösungen einsetzen möchte. Die mögliche mit dem Einsatz von Cloud-Lösungen entstehende Abhängigkeit von der Anbieterin durch Lock-In-Effekte muss strategisch durchdacht werden. Dazu kommt der Kontrollverlust sowie die in Frage gestellte Datensouveränität.

Cloud Computing ist eine Auftragsdatenbearbeitung. Sie bringt grössere Risiken mit sich, als andere Auslagerungen. Dennoch verbleibt die Verantwortung beim Auftraggeber Staat. Die Gesetze sehen aus diesem Grund klare Voraussetzungen für die grundsätzlich zulässige Auf-

tragsdatenbearbeitung vor. Es sind zusammengefasst zwei Bedingungen, die erfüllt sein müssen, damit in die Cloud ausgelagert werden kann. Es dürfen keine rechtlichen Bestimmungen entgegenstehen und die Verantwortung des Auftraggebers muss wahrgenommen werden. Beim ersten Punkt stehen Geheimnispflichten im Vordergrund. So ist durch die staatliche Institution zu prüfen, ob das Amtsgeheimnis, ein allfälliges besonderes Amtsgeheimnis oder Berufsgeheimnis der Auslagerung entgegenstehen. Des Weiteren kann eine vertragliche Vereinbarung entgegenstehen, eine Klassifizierung von Informationen oder weitere Regelungen. Steht eine rechtliche Bestimmung entgegen, kann geprüft werden, ob eine technische Massnahme die Kenntnisnahme verhindern kann. Ist dies der Fall (beispielsweise, wenn die Informationen verschlüsselt werden und das Schlüsselmanagement bei der öffentlichen Institution verbleibt, wenn die Personendaten anonymisiert oder pseudonymisiert werden), kann dennoch ausgelagert werden. Die zweite Bedingung erfordert, dass die staatliche Institution bei der Auswahl der Auftragsnehmerin ihre Sorgfaltspflicht wahrnimmt, vertraglich mit ihr die vorgegebenen Themen vereinbart und sich vergewissert, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann.

Bei der Auslagerung in die Cloud ist methodisch sauber vorzugehen. So sind im Rahmen der Rechtsgrundlagenanalyse die juristischen Fragen zu adressieren. Die Schutzbedarfs- und Risikoanalyse zeigt die erforderlichen Massnahmen auf, die im ISDS-Konzept behandelt werden. Das Datenschutzrecht sieht zudem die Durchführung einer Datenschutz-Folgenabschätzung vor. Ergibt diese, das besondere Risiken für die betroffenen Personen vorliegen, ist das Projekt der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

Beim Einsatz von Cloud-Lösungen spielt – wenn die Anbieterin eine US-amerikanische Unternehmung ist – zudem der CLOUD Act eine Rolle. Diese amerikanische Gesetzgebung verstösst gegen den ordre public der Schweiz. In diesen Fällen ist die Kenntnisnahme mittels technischer Lösungen (Verschlüsselung mit Schlüsselmanagement beim Auftraggeber, Anonymisierung oder Pseudonymisierung) auszuschliessen. Wenn dies nicht möglich ist, ist die Auslagerung bei Anwendbarkeit des Berufsgeheimnisses sowie von besonderen Amtsgeheimnissen ausgeschlossen. Bei Vorliegen des Amtsgeheimnisses müssen angemessene organisatorisch-technische Massnahmen ergriffen werden. Besonders schützenswerte Personendaten erfordern in diesem Fall auch eine Verschlüsselung mit Schlüsselmanagement bei der öffentlichen Institution.

Im Zusammenhang mit dem CLOUD Act wird fälschlicherweise festgehalten, es könne anhand einer Wahrscheinlichkeitsberechnungen der sich stellenden rechtlichen Frage begegnet werden. Damit wird verkannt, dass ein öffentliches Organ das Recht immer zu beachten und sich rechtmässig zu verhalten hat (Legalitätsprinzip), und andererseits kann das Verhalten einer amerikanischen Strafbehörde mit einer Methode mit Wahrscheinlichkeitsberechnungen nicht vorausgesagt werden. Nicht eingehaltenes Recht kann nicht durch tiefe Wahrscheinlichkeiten geheilt werden.

Clouds everywhere? Ja, aber rechtskonform und mit Durchblick trotz nebligem Himmel!

Literaturverzeichnis

BRUNO BAERISWYL, Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht, in: digma 2019, S. 118-122.

BRUNO BAERISWYL, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023.

EVA MARIA BELSER, § 5 Die Kompetenzverteilung zwischen Bund und Kantonen, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Stämpfli 2011.

ARTHUR BENZ, Der moderne Staat. Grundlagen der politologischen Analyse, 2. Aufl., De Gruyter 2008.

VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012.

DOMINIKA BLONSKI, Cloud Computing. Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Künstliche Intelligenz und Datenschutz. L'intelligence artificielle et protection des données, Tagungsband zum Dreizehnten Schweizerischen Datenschutzrechtstag, 2. Oktober 2020, Universität Fribourg, Schulthess 2021, S. 65 ff.

DOMINIKA BLONSKI, Was bedeutet die Revision für die kantonalen Datenschutzgesetze?, in: Astrid Epiney/Sophie Moser/Sophia Rovelli (Hrsg.), Die Revision des Datenschutzgesetzes des Bundes. La révision de la Loi fédérale sur la protection des données, Tagungsband zum Vierzehnten Schweizerischen Datenschutzrechtstag, 10. September 2021, Universität Fribourg, Schulthess 2022, S. 89 ff.

BUNDESAMT FÜR JUSTIZ, Bericht zum US CLOUD Act, 17. September 2021.

DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Merkblatt Cloud Computing, V 1.6 / Juli 2022, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf> (zuletzt besucht am 29.04.2023).

DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung – unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten, V 2.3 / Juli 2022, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

DATENSCHUTZBEAUFTRAGTE DES KANTONS ZÜRICH, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 29.04.2023).

DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Leitfaden «Auftragsdatenbearbeitung» (Bearbeitenlassen von Personendaten durch Dritte, § 7 IDG), V 1.0 / 08.04.2016, abrufbar unter: <https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html> (zuletzt besucht am 29.04.2023).

PETER FORSTMOSER/HANS-UELI VOGT, Einführung in das Recht, 5. Aufl., Stämpfli 2012.

ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER/DANIELA THURNHERR, Schweizerisches Bundesstaatsrecht, 10. Aufl., Schulthess 2020.

TOBIAS JAAG/LAURA BUCHER/RETO HÄGGI FURRER, Staatsrecht der Schweiz. in a nutshell, 2. Aufl., Dike 2016.

GERRY JOHNSON/RICHARD WHITTINGTON/KEVAN SCHOLES/DUCAN ANGWIN/PATRICK REGNÉR, Strategisches Management. Eine Einführung, 11. Aufl., Pearson 2018.

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), The NIST Definition of Cloud Computing, Special Publication 800-145, 2011, abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (zuletzt besucht am 29.04.2023).

PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, V 3.0 / 03.02.2022, abrufbar unter: <https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf> (zuletzt besucht am 29.04.2023).

PIERRE TSCHANNEN/ULRICH ZIMMERLI/MARKUS MÜLLER, Allgemeines Verwaltungsrecht, 4. Aufl., Stämpfli 2014.

AXEL TSCHENTSCHER/ANDREAS LIENHARD/FRANZISKA SPRECHER, Öffentliches Recht. Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., Dike 2019.

WOLFGANG WOHLERS, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015.

Rechtsquellenverzeichnis

BöB	Bundesgesetz über das öffentliche Beschaffungswesen vom 21. Juni 2019, SR 172.056.1
BV	Bundesverfassung der Schweizerischen Eigenossenschaft vom 18. April 1999, SR 101
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
DSG	Bundesgesetz über den Datenschutz vom 25. September 2020, SR 235.1
EPDV	Verordnung über das elektronische Patientendossier vom 22. März 2017, SR 816.11
GesG	Gesundheitsgesetz des Kantons Zürich vom 2. April 2007, LS 810.1
IDG	Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12. Februar 2007, LS 170.4
IDV	Verordnung über die Information und den Datenschutz des Kantons Zürich vom 28. Mai 2008, LS 170.41
ISG	Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz), SR 128
IVöB	Interkantonale Vereinbarung über das öffentliche Beschaffungswesen vom 15. März 2001
Konvention 108	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, SR 0.235.1
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 2011, SR 220
Org-VöB	Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung vom 24. Oktober 2012, SR 172.056.15

PG	Personalgesetz des Kantons Zürich vom 27. September 1998, LS 177.10
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
VöB	Verordnung über das öffentliche Beschaffungswesen vom 12. Februar 2020, SR 172.056.11
WTO-GPA	Revidiertes Übereinkommen über das öffentliche Beschaffungswesen vom 15. April 1994, SR 0.632.231.422

Selbstständigkeitserklärung

Ich erkläre hiermit, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls die Arbeit als nicht erfüllt bzw. mit Note 1 bewertet wird und dass die Universitätsleitung bzw. der Senat zum Entzug des aufgrund dieser Arbeit verliehenen Abschlusses bzw. Titels berechtigt ist.

Für die Zwecke der Begutachtung und der Überprüfung der Einhaltung der Selbstständigkeitserklärung bzw. der Reglemente betreffend Plagiate erteile ich der Universität Bern das Recht, die dazu erforderlichen Personendaten zu bearbeiten und Nutzungshandlungen vorzunehmen, insbesondere die schriftliche Arbeit zu vervielfältigen und dauerhaft in einer Datenbank zu speichern sowie diese zur Überprüfung von Arbeiten Dritter zu verwenden oder hierzu zur Verfügung zu stellen.

Zürich, 29. April 2023 Dominika Blonski

Über die Autorin

Dominika Blonski absolvierte das Studium der Rechtswissenschaften an der Universität Fribourg. Im Rahmen ihrer Dissertation an der Universität Bern verbrachte sie Nationalfonds-Forschungsaufenthalte an der New York University in New York und an der Jagiellonen Universität in Krakau. Sie promovierte zum Thema «Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts» (Professor-Walther-Hug-Preis). Mit dem CAS in Information Security – Management der Hochschule Luzern erweiterte die Juristin ihre interdisziplinären Kompetenzen in den Bereichen Informationssicherheits-Management und Technik.

Nach ihrer Tätigkeit als wissenschaftliche Assistentin an der Universität Bern folgte ab 2014 ihre Tätigkeit beim Datenschutzbeauftragten des Kantons Zürich, zuletzt als Leiterin der Abteilung Recht und Informationssicherheit. Dominika Blonski wurde im Dezember 2019 vom Kantonsrat zur neuen Datenschutzbeauftragten des Kantons Zürich gewählt und ist seit dem 1. Mai 2020 im Amt. Sie ist Mitglied des Büros (Vorstand) von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Zudem ist sie Dozentin verschiedener Kurse (z.B. an der zhaw), Mitherausgeberin zweier Kommentare zum Datenschutzrecht und Autorin von Publikationen in Fachzeitschriften.