HOCHSCHULE FÜR
ÖFFENTLICHE VERWALTUNG UND FINANZEN
LUDWIGSBURG

UNIVERSITY OF APPLIED SCIENCES

HOCHSCHULE FÜR ÖFFENTLICHE VERWALTUNG UND FINANZEN LUDWIGSBURG

Datenschutz im öffentlichen Sektor:

Eine umfassende Untersuchung der Datenschutzaspekte in öffentlichen Institutionen unter Berücksichtigung der wachsenden Verwendung digitaler Technologien und Cloud-Services

Bachelorarbeit

Zur Erlangung des Grades eines Bachelor of Arts (B. A.) im Studiengang gehobener Verwaltungsdienst – Public Management

Vorgelegt von

Alina Sarah Kopf

Studienjahr 2024/2025

Erstgutachter: Herr Dipl. Verw. Wiss. Martin Brandt

Zweitgutachter: Herr Daniel Kanthaus, LL. B.

Genderhinweis

Aus Gründen der leichteren Lesbarkeit wird in der vorliegenden Arbeit die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen oder diversen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AWS	Amazon Web Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BDSG	Bundesdatenschutzgesetz
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EDV	Elektronische Datenverarbeitung
ENISA	European Union Agency for Cybersecurity
EU	Europäische Union
ISO	International Organization for Standardization
IT	Informationstechnik
LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SECaaS	Security as a Service
SSD	Solid State Disk
StGB	Strafgesetzbuch
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen
U. S.	United States
VPN	Virtual Private Network

Abbildungsverzeichnis

Verzeichnis der Anlagen

1. Einleitung

In einer zunehmend digitalisierten Welt, in der personenbezogene Daten in vielfältigen digitalen Netzwerken verarbeitet werden, wird der Schutz dieser Informationen zu einer immer dringlicheren Herausforderung. Der öffentliche Sektor erfasst und verarbeitet personenbezogene Daten umfassend, von grundlegenden Identifikationsinformationen bis hin zu sensiblen medizinischen und sozialen Angaben. Diese Datenverarbeitung beginnt mit der Ausstellung der Geburtsurkunde und begleitet uns durch sämtliche Lebensabschnitte, wobei sie eine zentrale Rolle in der Erfüllung zahlreicher öffentlicher Aufgaben spielt.

Mit dem Ziel, Verwaltungsprozesse elektronisch abzuwickeln, um bürgernah, effizient und transparent zu agieren, wurden als rechtliche Grundlage in Deutschland das E-Government-Gesetz und das Onlinezugangsgesetz erlassen. Diese Gesetze fordern die Verwaltung nicht nur zur elektronischen Aktenführung auf, sie legen zudem fest, wie die öffentliche Verwaltung mit den Bürgern und Unternehmen digital kommunizieren soll, einschließlich elektronischer Formulare.[1]

Um diese Anforderungen effektiv umzusetzen, bedarf es leistungsfähiger IT-Infrastrukturen, die flexibel und sicher sind. An dieser Stelle rückt das Thema Cloud-Computing in den Fokus. Cloud-Computing bietet die technologische Grundlage, um die gesetzlichen Vorgaben zu erfüllen, indem es ermöglicht, digitale Dienste effizient bereitzustellen und zu verwalten. Es stellt damit eine zentrale Komponente der digitalen Transformation in der öffentlichen Verwaltung dar und eröffnet neue Möglichkeiten für Verwaltungsprozesse. Allerdings bringt die Nutzung von Cloud-Services auch besondere Herausforderungen mit sich, insbesondere im Hinblick auf den Datenschutz. Da in öffentlichen Institutionen sensible Daten verarbeitet werden, ist die Implementierung strenger Datenschutzmaßnahmen unerlässlich. Nur so kann gewährleistet werden, dass die Daten sicher verarbeitet werden und den gesetzlichen Vorgaben der Datenschutz-Grundverordnung (DSGVO) entsprechen. Ein robuster Datenschutz in der Cloud ist daher nicht nur eine rechtliche Notwendigkeit, sondern auch entscheidend für das Vertrauen der Bürger in digitale

[1] Vgl. § 6a EGovG.

Verwaltungsdienste. Diese Arbeit soll einen Beitrag dazu leisten, das Bewusstsein für die Erforderlichkeit eines robusten Datenschutzmanagements bei der Verwendung von Cloud-Diensten zu schärfen und praxisorientierte Maßnahmen aufzeigen, die den gesetzlichen Anforderungen gerecht werden.

1.1 Problemstellung

Die Nutzung von Cloud-Technologien in öffentlichen Institutionen bringt spezifische Datenschutzrisiken mit sich, insbesondere in Bezug auf die Kontrolle über die Datenverarbeitung und den Schutz sensibler Informationen. Cloud-Services werden häufig von Drittanbietern mit global verteilten Rechenzentren betrieben, was das Risiko unbefugter Zugriffe und die Übertragung von Daten in Länder birgt, die nicht den strengen Anforderungen der DSGVO entsprechen. Das zentrale Problem besteht darin, dass bei der Auslagerung von Daten in die Cloud die Einhaltung der DSGVO gefährdet sein kann, insbesondere wenn die Datenverarbeitung außerhalb der Europäischen Union erfolgt und die Kontrollmöglichkeiten der öffentlichen Institutionen eingeschränkt sind.

1.2 Zielsetzung der Arbeit

Vor diesem Hintergrund strebt diese Arbeit an, eine umfassende Analyse der Datenschutzaspekte im Kontext von Cloud-Diensten im öffentlichen Sektor durchzuführen. Der Schwerpunkt liegt darauf, wirksame Maßnahmen zu ermitteln und darzustellen, die den Schutz sensibler Daten und die Einhaltung geltender Datenschutzbestimmungen in dieser zunehmend digitalisierten Umgebung gewährleisten. Diese Arbeit soll auch als Leitfaden für öffentliche Institutionen dienen, die sich noch am Anfang ihrer Auseinandersetzung mit Cloud-Computing befinden. Als praxisnahe Hilfestellung werden eigens erstellte Checklisten verwendet, die in der Praxis als Unterstützung bei der Entscheidung über eine Auslagerung der Daten in die Cloud eingesetzt werden können.

1.3 Forschungsfragen

Um diese Zielsetzung zu erreichen, fokussiert sich die Arbeit auf die Beantwortung folgender Fragen:

Welche spezifischen Risiken und Herausforderungen bestehen im Zusammenhang mit Datenschutz in der Cloud im öffentlichen Sektor?

Welche technischen und organisatorischen Maßnahmen sind besonders gut geeignet, um einen effektiven Datenschutz in der Cloud zu gewährleisten und die Integrität sensibler Daten zu bewahren?

Wie kann die Cloud-Technologie im öffentlichen Sektor trotz dieser Herausforderungen effektiv genutzt werden, um die Digitalisierung voranzutreiben, ohne dabei die datenschutzrechtlichen Anforderungen zu gefährden?

1.4 Aufbau der Arbeit

Im ersten Teil werden die Grundlagen des Datenschutzrechts behandelt. Dabei wird auf die essenziellen Datenschutzgrundsätze eingegangen, wie etwa die Vertraulichkeit, Integrität und Transparenz.

Anschließend erfolgt eine umfassende Einführung in die Grundlagen des Cloud-Computings. Dies umfasst nicht nur eine Definition des Begriffs, sondern auch eine detaillierte Betrachtung der verschiedenen Bereitstellungs- und Servicemodelle. Zudem werden die damit verbundenen Vorteile sowie die potenziellen Risiken und Herausforderungen, die innerhalb dieser Modelle existieren, thematisiert.

Der zweite Teil widmet sich den praktischen Aspekten des Datenschutzes in der Cloud. Hier stehen die organisatorischen und technischen Maßnahmen im Fokus, die zur Gewährleistung eines angemessenen Schutzes personenbezogener Daten unerlässlich sind. Es wird dargelegt, welche Maßnahmen erforderlich sind, um möglichen Risiken entgegenzuwirken und wie eine digitale Atmosphäre gestaltet werden kann, die den Datenschutz gewährleistet. Abschließend wird beurteilt, ob Cloud-Computing im öffentlichen Sektor Zukunftspotenzial hat und in einem Fazit werden die gewonnenen Erkenntnisse zusammengefasst.

2. Datenschutzgrundsätze

Um die Datenschutzaspekte im Cloud-Computing wirksam analysieren zu können, ist es entscheidend, zunächst die grundlegenden Datenschutzprinzipien zu verstehen, die in Art. 5 Abs. 1 DSGVO verankert sind. Diese Prinzipien definieren den Rahmen für die rechtmäßige Verarbeitung personenbezogener Daten, die alle Informationen umfassen, die eine identifizierbare natürliche Person betreffen.[2] Im Kontext von Cloud-Computing, wo Daten oft in globalen und dynamischen Umgebungen verarbeitet werden, stellen diese Grundsätze eine wichtige Grundlage für den Schutz der Privatsphäre dar. Der Begriff "Verarbeitung" beschreibt jegliche Handlung oder Abfolge von Handlungen, ob automatisiert oder nicht, die im Zusammenhang mit personenbezogenen Daten stehen, wie z. B. das Speichern.[3]

2.1 Rechtmäßigkeit und Transparenz

Die Prinzipien der Rechtmäßigkeit und Transparenz sind zentrale Elemente des Datenschutzes und besonders relevant im Kontext von Cloud-Computing.[4] Daten dürfen nicht automatisiert weiterverarbeitet und ggf. auf Servern gespeichert werden, auf welchen eine Speicherung nicht rechtmäßig ist. Die Verarbeitung ist nur dann rechtmäßig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Einwilligung der betroffenen Person,
- Erfüllung eines Vertrags,
- gesetzliche Verpflichtung,
- Schutz lebenswichtiger Interessen,
- Ausführung einer Aufgabe im öffentlichen Interesse oder Wahrung berechtigter Interessen.[5]

[2] Vgl. Art. 4 Nr. 1 DSGVO.
[3] Vgl. Art. 4 Nr. 2 DSGVO.
[4] Vgl. Art. 5 Abs. 1 lit. a DSGVO .
[5] Vgl. Art. 6 I DSGVO.

Zudem müssen die Anforderungen an die Transparenz gemäß Art. 13 und 14 DSGVO gewährleistet sein. Transparenz bedeutet, dass Nutzer klar und verständlich darüber informiert werden müssen, wo und wie ihre Daten verarbeitet werden, um so Vertrauen in die Cloud-Services zu schaffen.

2.2 Zweckbindung

Der Verantwortliche[6] muss sicherstellen, dass Daten nur für festgelegte, klare und legitime Zwecke erhoben werden.[7] Diese Daten dürfen nicht in einer Weise weiterverarbeitet werden, die diesen Zwecken widerspricht. Öffentliche Institutionen sowie Cloud-Anbieter müssen strikt darauf achten, dass die Verarbeitung nur die Daten, die für die Erreichung der Zwecke notwendig sind, umfasst. Behörden müssen genau festlegen, zu welchen Zwecken ihre Daten in der Cloud verarbeitet werden. Diese Zwecke dürfen nicht ohne ihre Zustimmung geändert werden. Sollte eine weitere Verarbeitung geplant sein, muss sichergestellt werden, dass die neuen Zwecke mit den ursprünglichen vereinbar sind, wie in Artikel 6 Absatz 4 DSGVO festgelegt.[8]

2.3 Datenminimierung

Das Prinzip der Datenminimierung besagt, dass nur die Daten erhoben werden dürfen, die für den jeweiligen Zweck notwendig sind.[9] In Cloud-Umgebungen bedeutet dies, dass die Menge der verarbeiteten Daten auf das erforderliche Minimum reduziert werden muss. Techniken wie Anonymisierung und Pseudonymisierung können dabei helfen, die Menge personenbezogener Daten zu minimieren und somit das Risiko für die Betroffenen zu reduzieren.

---

[6] Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. In Bezug auf diese Arbeit kann stets von der öffentlichen Institution als Verantwortlichen ausgegangen werden.

[7] Vgl. Art. 5 Abs. 1 lit. b DSGVO.

[8] Vgl. Spiecker/Bretthauer, Dokumentation zum Datenschutz, Rn. 71.

[9] Vgl. Art. 5 Abs. 1 lit. c DSGVO.

2.4 Richtigkeit und Aktualität

Die Richtigkeit und Aktualität personenbezogener Daten sind in Cloud-Umgebungen von besonderer Bedeutung, da Daten oft über mehrere Standorte hinweg synchronisiert werden.[10] Um sicherzustellen, dass die Daten korrekt und aktuell bleiben, müssen Mechanismen zur regelmäßigen Überprüfung und Aktualisierung der Daten implementiert werden. Besonders bei der Nutzung von Backups ist es essenziell, dass diese regelmäßig mit den neuesten Datenständen synchronisiert werden, um die Integrität der Informationen zu gewährleisten.

2.5 Speicherbegrenzung und Löschung

Das Prinzip der Speicherbegrenzung verlangt, dass personenbezogene Daten nur so lange gespeichert werden, wie es für die Erreichung der Verarbeitungszwecke notwendig ist.[11] In Cloud-Umgebungen ist die vollständige und endgültige Löschung von Daten eine besondere Herausforderung, da diese oft in verteilten Systemen und auf mehreren Servern gespeichert werden. Es müssen deshalb Mechanismen entwickelt werden, die sicherstellen, dass personenbezogene Daten vollständig und zuverlässig auf allen betroffenen Servern gelöscht werden können.

2.6 Integrität und Vertraulichkeit

Integrität und Vertraulichkeit sind zentrale Prinzipien des Datenschutzes, die im Cloud-Computing durch geeignete technische und organisatorische Maßnahmen gewährleistet werden müssen.[12] Das Urteil des Bundesverfassungsgerichts aus dem Jahr 2008 definiert „Vertraulichkeit“ als den Schutz vor unbefugtem Zugriff auf vorhandene Daten und „Integrität“ als den Schutz vor der Manipulation dieser Daten.[13] Die Verarbeitung der personenbezogenen Daten sollte durch angemessene technische und organisatorische Maßnahmen erfolgen, um die Sicherheit dieser Daten zu gewährleisten. Dies beinhaltet den Schutz vor unbefugtem oder rechtswidrigem Zugriff sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schäden.

---

[10] Vgl. Art. 5 Abs. 1 lit. d DSGVO.
[11] Vgl. Art. 5 Abs. 1 lit. e DSGVO.
[12] Vgl. Art. 5 Abs. 1 lit. f DSGVO.
[13] Vgl. Bundesverfassungsgericht, Urteil vom 27. Februar 2008, 1 BvR 370/070, Rn. 1 – 333.

2.7 Rechenschaftspflicht

Der Grundsatz der Rechenschaftspflicht besagt, dass der Verantwortliche für die Einhaltung aller vorgenannten Grundsätze verantwortlich ist und die Wahrung dieser Grundsätze nachzuweisen hat.[14] Für Cloud-Dienstanbieter, welche gemäß Art. 4 Abs. 8 DSGVO als Auftragsverarbeiter eingestuft werden, da sie Daten des Verantwortlichen im Auftrag verarbeiten, geht keine ausdrückliche Rechenschaftspflicht aus Art. 5 DSGVO hervor. Allerdings kann eine solche aus Art. 28 Abs. 5 DSGVO – vergleichbar mit Art. 32 Abs. 3 DSGVO – abgeleitet werden, die vorsieht, dass die Verantwortlichkeit für die Einhaltung der Datenschutzanforderungen auch auf die Auftragsverarbeiter übertragen werden kann. Dies bedeutet, dass Cloud-Anbieter entsprechende Nachweise erbringen müssen.

Um zu verstehen, wie diese Grundsätze in Cloud-Umgebungen umgesetzt werden können, muss zunächst klar sein, was unter Cloud-Computing zu verstehen ist und welche Möglichkeiten es bietet. Im nächsten Abschnitt wird daher erklärt was Cloud-Computing ist und welche grundlegenden Charakteristika es besitzt.

3. Definition und Grundlagen des Cloud-Computings

Cloud-Computing bezeichnet die Nutzung von IT-Ressourcen wie Speicherplatz, Rechenleistung und Anwendungen über das Internet. Nach der Definition des National Institute of Standards and Technology (NIST) ist Cloud Computing ein Modell, das den Netzwerkzugriff auf einen gemeinsam nutzbaren Pool konfigurierbarer Rechenressourcen (z. B. Netzwerke, Server, Speicher, Anwendungen und Dienste) ermöglicht. Diese Ressourcen sollen schnell bereitgestellt und mit minimalem Verwaltungsaufwand freigegeben werden können.[15] Statt eigene Hardware oder Software zu besitzen und zu betreiben, greifen Nutzer auf externe Speicher zu, die von einem Drittanbieter bereitgestellt werden. Dies ermöglicht den Zugriff auf Daten über ein Netzwerk von überall aus, ohne dass physische Hardware lokal vorhanden sein muss. Ein bekanntes Beispiel für Cloud-Computing ist die Nutzung

[14] Vgl. Art. 5 Abs. 2 DSGVO.
[15] Vgl. Grance/Mell, NIST Special Publication 800-145, S. 2, Anlage 1.

von Google Drive, wo Benutzer Dateien online speichern und von verschiedenen Geräten aus darauf zugreifen können.

Als die fünf grundlegenden Charakteristika von Cloud Computing benennt das NIST „On-demand self-service“, „Broad network access“, „Resource pooling“, „Rapid elasticity“ sowie „Measured service“. In der Welt des Cloud-Computing bedeutet „On-demand“, dass Benutzer jederzeit und nach Bedarf auf spezifische IT-Ressourcen zugreifen können und zwar ganz ohne lange Vorlaufzeiten oder manuelle Prozesse zur Bereitstellung dieser Ressourcen. Die Zurverfügungstellung der IT-Ressourcen läuft automatisch und eine Interaktion mit dem Cloud-Service-Provider ist nicht nötig.[16] „Broad network access“ steht für die Verfügbarkeit der Funktionen über das Netzwerk. Der Zugriff erfolgt über Standardmechanismen, die die Verwendung heterogener Endgeräte erlauben (z. B. Notebook, PC, Tablet-PC oder Smartphone). „Resource pooling“ beschreibt, dass die Rechenressourcen des Anbieters nach dem „multi-tenant-modell“ zusammengelegt werden, um mehrere Nutzer zu bedienen. Dieses Modell ermöglicht es, dass sich mehrere Nutzer dieselbe Softwareanwendung teilen, während ihre Daten und Konfigurationen getrennt bleiben. Dabei werden verschiedene physische und virtuelle Ressourcen je nach Bedarf der Nutzer dynamisch zugewiesen. Die genaue Lage der bereitgestellten Ressourcen ist für den Kunden normalerweise nicht bekannt oder steuerbar, jedoch kann auf einer höheren Abstraktionsebene (z. B. Land, Bundesland oder Rechenzentrum) eine Standortwahl möglich sein. Die vierte Eigenschaft „Rapid elasticity“, beschreibt die Fähigkeit, Ressourcen elastisch und schnell – in manchen Fällen automatisch – je nach Bedarf zu skalieren. Im Kontext von Cloud-Computing bezeichnet „elastisch“ die Fähigkeit eines Systems, seine Ressourcen dynamisch und flexibel an den aktuellen Bedarf anzupassen. Das bedeutet, dass die IT-Ressourcen wie Rechenleistung, Speicherplatz oder Bandbreite schnell und automatisch vergrößert oder verkleinert werden können, je nachdem, wie stark die Nachfrage steigt oder fällt. Skalieren bezeichnet dabei den Prozess der Anpassung

[16] Vgl. Kosmides, in: Schneider (Hrsg.), Handbuch EDV-Recht, W. Vertragsrecht der Internet-Dienstleistungen, Rn. 565.

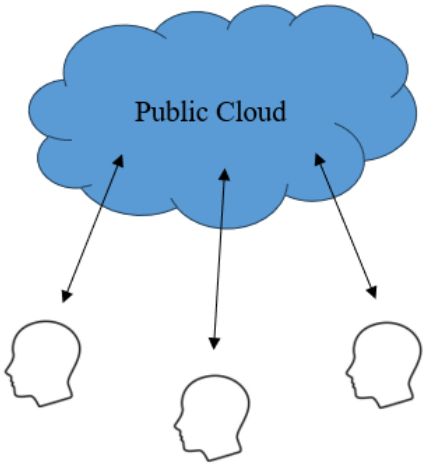
der Kapazität und Leistung eines Systems. „Measured service“ steht für die automatische Überwachung und Verbesserung der Ressourcennutzung, indem Cloud-Systeme Parameter messen, die abhängig vom jeweiligen Service sind, wie beispielsweise Datenspeicher, Rechenleistung, Bandbreite und aktive Nutzerzahlen.[17]

3.2 Bereitstellungsmodelle

Ein wesentliches Element des Cloud-Computings sind die verschiedenen Bereitstellungsmodelle, die festlegen, wie Cloud-Dienste zur Verfügung gestellt und genutzt werden. Diese Modelle bestimmen, wie Infrastruktur, Plattformen und Software organisiert und verwaltet werden und bieten unterschiedliche Grade der Kontrolle und Skalierbarkeit. Ein detailliertes Verständnis dieser Modelle ist entscheidend, um die besten Lösungen für spezifische Anforderungen auszuwählen und die Vorteile der Cloud-Technologie optimal nutzen zu können.

3.2.1 Public Cloud

Public Clouds repräsentieren allgemein zugängliche Commodity-Dienstleistungen, die vollständig automatisiert sind. Unter Commodity-Dienstleistungen versteht man standardisierte Dienstleistungen, die in der Regel als Massenprodukte oder Massendienste betrachtet werden können.[18] Sie sind für die breite Öffentlichkeit zugänglich und richten sich an einen offenen Nutzerkreis. Das bedeutet, dass sie jedermann nutzen kann und dass es keine spezifischen Abhängigkeiten oder rechtliche Beziehungen zwischen dem Cloud-Anbieter und dem Kunden, die über die bloße Bezugsvereinbarung hinausgeht, gibt.[19] Die Nutzer agieren in der



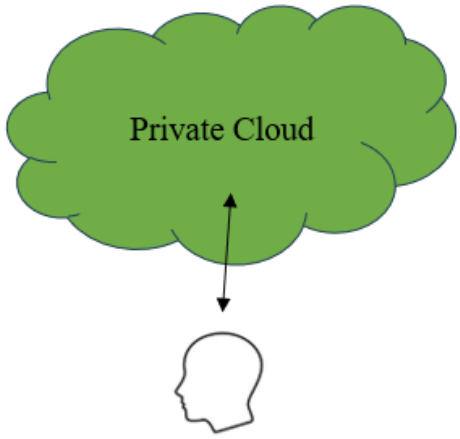
Quelle: Eigene Darstellung

[17] Vgl. Grance/Mell, NIST Special Publication 800-145, S. 2, Anlage 1.
[18] Vgl. Committee on National Security Systems, Glossary, CNSSI No. 4009, S. 21, Anlage 2.
[19] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 66.

Regel unabhängig voneinander und es bestehen keine organisatorischen Verbindungen untereinander. Der Fokus liegt auf der gemeinsamen Nutzung von Ressourcen, insbesondere Server- und Speicherressourcen.[20] Die Public Cloud bietet dadurch ein hohes Maß an Flexibilität, da sich die Kapazität nach Bedarf anpassen lässt. Die allgemeine Zugänglichkeit und die gemeinsame Nutzung der zugrunde liegenden Ressourcen durch eine unbestimmte Anzahl von Nutzern verleihen den Aspekten des Datenschutzes und der Datensicherheit in Public Clouds besondere Bedeutung. Beispiele für Public Clouds sind Amazon Web Services (AWS), Microsoft Azure oder die Google Cloud Platform, welche eine Vielzahl von Diensten wie z. B. Rechenleistung oder Speicher anbieten.[21]

3.2.2 Private Cloud

Bei Private Clouds handelt es sich um Cloud-Umgebungen, die nicht für die breite Öffentlichkeit zugänglich sind. Sie stehen stattdessen ausschließlich einem spezifischen, im Voraus festgelegten Nutzerkreis zur Verfügung, wie beispielsweise den Mitarbeitern einer Behörde und bieten dadurch eine erhöhte Datensicherheit. Lediglich befugte Nutzer der Cloud können auf die gemeinsam bereitgestellten Ressourcen zugreifen, beispielsweise über ein Intranet oder ein Virtual Private Network.[22]



Quelle: Eigene Darstellung

Der Betrieb und die Verwaltung erfolgen durch eine zentrale Instanz, das sogenannte Shared Service Center. Diese stellen IT-Dienstleistungen für teilnehmende Einheiten bereit und verwalten und berechnen die Nutzung. Dieses Modell wird auch als internes Outsourcing bezeichnet. In der Regel verschmelzen Nutzer und

[20] Vgl. Hennrich in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S. 460, Rn. 15.
[21] Vgl. Hennrich, Cloud-Computing nach der Datenschutz-Grundverordnung, S. 39 - 41.
[22] Vgl. Hennrich in: Seckelmann (Hrsg.), Digitalisierte Verwaltung Vernetztes E-Government, S. 460, Rn. 16.

Anbieter und die Trennung zwischen IT-Dienstleistern/Anbietern und Nutzern/Kunden wird in diesem selbstversorgungsähnlichen Bereich weitgehend aufgehoben.[23]

3.2.3 Community Cloud

Die Community Cloud repräsentiert einen Zusammenschluss mehrerer Private Clouds unterschiedlicher Organisationen, die ein gemeinsames Netzwerk bilden. Die Festlegung der Nutzungsbedingungen erfolgt gemeinschaftlich, wobei individuelle Vereinbarungen bestimmte Ressourcen oder Nutzungsmerkmale aus spezifischen Private Clouds betreffen können. Diese Art von Cloud-Modell findet Anwendung im Bereich von Verbänden, Institutionen, der Verwaltung und generell in Situationen, in denen verschiedene Organisationen mit ähnlichen Interessen, wie beispielsweise Sicherheits- oder Compliance-Anforderungen, kooperativ zusammenarbeiten. Dabei stehen sie nicht im direkten Wettbewerb und können die Cloud-Infrastruktur aufgrund gemeinsamer regulatorischer Vorgaben teilen.[24]

3.2.4 Externe und interne Cloud

Externe und interne Clouds unterscheiden sich in Bezug auf Nutzerzugriff, physischen Standort und Implementierung. Diese Modelle haben dadurch Auswirkungen auf die Kontrolle, Sicherheit und Flexibilität von IT-Ressourcen im öffentlichen Sektor.[25]

Interne Clouds entsprechen dem Intranet und sind lokal gehostet. Der Zugriff ist auf authentifizierte, behördeninterne Nutzer beschränkt. Die Behörde ist Eigentümerin der physischen Infrastruktur. Anwenderdaten verbleiben im Haus intern, was den Sicherheits- und Datenschutzanforderungen sehr dienlich ist. Das Modell ermöglicht eine umfassende Kontrolle über die IT-Ressourcen, birgt jedoch den

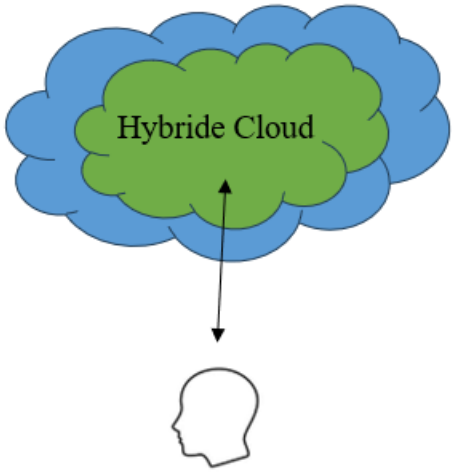
[23] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 68.
[24] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 74 – 75.
[25] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 71.

Nachteil, dass es die Skalierbarkeit einschränken kann, da nur die vor Ort befindlichen Ressourcen genutzt werden können. Eine interne Cloud ist zwangsläufig auch eine Private Cloud, da sie innerhalb der organisatorischen Grenzen genutzt wird.[26]

Im Gegensatz dazu bezieht die externe Cloud IT-Infrastruktur von Drittanbietern oder externen Dienstleistern. Der Zugriff erfolgt von außen und die physische Kontrolle über die Infrastruktur liegt nicht beim Nutzer. Dieses Modell ist nicht zwangsläufig eine Public Cloud, aber eine Public Cloud ist aufgrund der Nutzung externer Ressourcen immer eine externe Cloud. Es bietet Skalierbarkeit und Flexibilität, geht jedoch mit geringerer Kontrolle einher.[27]

3.2.5 Hybride Cloud

Die Hybridnutzung von internen und externen Ressourcen bietet eine vielseitige Lösung, die den individuellen Bedürfnissen gerecht werden kann. Hybride Clouds kombinieren Elemente sowohl aus Private- als auch Public-Cloud-Modellen, wobei typischerweise eine Public Cloud mit einer Private Cloud verknüpft wird. Diese Modelle bleiben in der Regel eigenständige Einheiten, werden jedoch durch Middleware-Software verbunden, um den Austausch von Daten und Anwendungen zu ermöglichen. Diese Herangehensweise vereint die kosteneffiziente Skalierbarkeit einer Public Cloud mit den Sicherheits- und Kontrollaspekten einer Private Cloud.[28]



Quelle: Eigene Darstellung

Ein spezielles Hybridmodell ist die Virtual Private Cloud, bei der die Netzwerk- und Ressourcenumgebung einer Public Cloud genutzt wird, jedoch durch Isolati-

[26] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 72 – 73.
[27] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 72.
[28] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 76 – 77.

onstechniken eine Private Cloud mit begrenzten Zugriffsrechten entsteht. Eine Virtual Private Cloud ist daher ein Single-Tenant-Modell, da es die Möglichkeit bietet, einen privaten Bereich innerhalb der Architektur einer Public Cloud einzurichten. Sie verfügt über ein höheres Maß an Sicherheit als traditionelle Multi-Tenant-Angebote für Public Clouds, ermöglicht es aber dennoch von der hohen Verfügbarkeit, Flexibilität und Kosteneffizienz, wie Public Clouds sie bieten, zu profitieren.[29] Ein Beispiel hierfür wäre AWS Outposts. Dabei wird AWS-Hardware direkt im Rechenzentrum des Nutzers installiert. Diese Hardware wird dann über eine sichere Verbindung mit der AWS-Cloud verbunden, sodass dann dieselben AWS-Dienste wie in der Cloud genutzt werden können, jedoch auf eigener, lokal installierter Hardware.[30]

3.2.6 Sealed Cloud

Eine Sealed Cloud ist eine patentierte Sicherheitstechnologie eines hochsicheren Cloud-Systems, das sich durch besonders strenge Sicherheitsvorkehrungen auszeichnet. Ein zentraler Aspekt dabei ist, dass der Cloud-Anbieter selbst keinen Zugriff auf die unverschlüsselten Daten hat, sodass nur der berechtigte Nutzer diese entschlüsseln und verwenden kann. Zudem wird in der Sealed Cloud eine durchgehende Ende-zu-Ende-Verschlüsselung angewendet, bei der die Daten bereits auf der Kundenseite verschlüsselt werden.[31] Dies stellt sicher, dass die Daten während der gesamten Verarbeitung geschützt sind. Ein weiteres Sicherheitsmerkmal ist die isolierte Datenverarbeitung, bei der Daten nur in verschlüsselten und isolierten Umgebungen verarbeitet werden. Eine Sealed Cloud eignet sich besonders für Anwendungen, bei denen die Sicherheit der Daten höchste Priorität hat, vor allem in Bereichen in denen sehr sensible Daten verarbeitet werden, wie im öffentlichen Sektor. Sie bietet eine Lösung für Behörden, die die Vorteile von Cloud-Computing

[29] Vgl. Fecke/Grupp, in: Ebers (Hrsg.), Legal Tech, Cloud Computing, allgemein, Rn. 78.
[30] Vgl. Hennrich, Cloud-Computing nach der Datenschutz-Grundverordnung, S. 44 - 45.
[31] Die verschiedenen Verschlüsselungsmethoden, wie die Ende-zu-Ende-Verschlüsselung, werden in dieser Arbeit unter „7.1.2 Verschlüsselung“ noch genauer behandelt.

nutzen wollen, aber keine Kompromisse bei der Sicherheit ihrer Daten eingehen können.[32]

3.3 Service-Modelle

Cloud Computing basiert auf der bedarfs- und nutzungsbasierten Bereitstellung von IT-Ressourcen, wie es durch die umfassende Definition des NIST verdeutlicht wird.[33] In einem Drei-Ebenen-Modell wird die Bereitstellung von Infrastruktur, Plattformen und Software grundlegend differenziert.[34]

3.3.1 Infrastructure as a Service

Auf der untersten Ebene dieses Modells, die sich auf die grundlegenden Infrastrukturkomponenten konzentriert, bietet Cloud Computing eine flexible und bedarfsorientierte Bereitstellung von IT-Infrastruktur als Dienst („as a Service“). Diese umfasst die Bereitstellung von Hardware-Ressourcen wie Rechenleistung, Arbeitsspeicher und Speicherplatz sowie Netzwerkkomponenten wie Router oder Switch, welche zur Realisierung des Internets notwendig sind. Die verbundenen Geräte tauschen über Netzwerkprotokolle Daten bzw. Informationen aus, indem sie miteinander kommunizieren. Diese Dienste ermöglichen es dem Nutzer, innerhalb der vom Anbieter bereitgestellten und in der Regel virtualisierten Infrastruktur, Betriebssysteme und Software nach eigenen Präferenzen auszuführen.[35]

3.3.2 Platform as a Service

Platform as a Servive (PaaS) befindet sich in der Mitte der dreischichtigen Service-Struktur des Cloud-Computings und wird oft als „Cloud-Betriebssystem“ bezeichnet. Es stellt Endbenutzern eine internetbasierte Umgebung für die Entwicklung von Anwendungen zur Verfügung, einschließlich Anwendungsprogrammierschnittstellen und Betriebssystemplattformen, also eingekapselte IT-Fähigkeiten oder

[32] Vgl. Uniscon GmbH, Sealed Cloud - Hochsichere Cloud-Lösungen sogar für Geheimnisträger gem. § 203 StGB, (o. S.), Anlage 3.
[33] Vgl. NIST, Special Publication 800-145, S. 2.
[34] Vgl. Hennrich in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S. 458, Rn. 9.
[35] Vgl. Hennrich in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S. 458 – 459, Rn. 10.

logische Ressourcen wie Datenbanken und Dateisysteme. Dabei unterstützt es verschiedene Software-/Hardware-Ressourcen und Tools, die für den gesamten Lebenszyklus von Anwendungen von der Erstellung bis zum Betrieb erforderlich sind.[36]

3.3.3 Software as a Service

Software as a Service (SaaS) ist der gängigste Cloud-Computing-Dienst und befindet sich an der obersten Ebene der dreistufigen Cloud-Computing-Dienstleistung. Die Bereitstellung des gesamten Spektrums an Anwendungssoftware erfolgt über einen Standard-Webbrowser im Internet. Diese Bandbreite reicht von Web-Applikationen bis zu komplexer Standardsoftware in Bereichen wie Office-Anwendungen, Finanzbuchhaltung oder Enterprise-Resource-Planning (ERP)-Lösungen. Unter einer solchen ERP-Lösung wird nach Hesseler und Görtz „eine integrierte Software verstanden, die auf Basis standardisierter Module für alle oder wesentliche Teile der Geschäftsprozesse eines Unternehmens aus betriebswirtschaftlicher Sicht informationstechnisch unterstützt. Die zur Verfügung stehenden Systemfunktionalitäten liefern dabei aktuelle Informationen auf Basis der erfassten und verarbeiteten Daten und ermöglichen hierdurch eine unternehmensweite Planung, Steuerung und Kontrolle.“[37] Beispiele für typische SaaS-Dienste sind Microsoft Office 365 oder Google Docs. Im öffentlichen Sektor spielt die Bereitstellung von Fachanwendungen eine zentrale Rolle auf der SaaS-Ebene. Hierbei handelt es sich um spezialisierte Anwendungen, die in verschiedenen Bereichen wie dem Gesundheits-, Bildungs- oder Sozialwesen eingesetzt werden.[38]

[36] Vgl. Huawei Technologies Co., Ltd., Cloud Computing Technology, S. 31.
[37] Hesseler/Görtz, Basiswissen ERP-Systeme, S 5 - 6.
[38] Vgl. Huawei Technologies Co., Ltd., Cloud Computing Technology, S. 33.

4. Datensicherheit und -schutz

Datenschutz und Datensicherheit sind zwei Schlüsselkonzepte im digitalen Zeitalter, die oft miteinander verwechselt werden, aber unterschiedliche Schwerpunkte setzen. Datensicherheit bezieht sich auf Maßnahmen und Technologien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten. Dies beinhaltet den Schutz vor unbefugtem Zugriff, Datenverlust, Diebstahl oder Beschädigung. Datenschutz bezieht sich auf den Schutz personenbezogener Daten und die Einhaltung der damit verbundenen gesetzlichen Bestimmungen und Vorschriften. Es geht darum, sicherzustellen, dass personenbezogene Informationen angemessen verarbeitet werden. Verfassungsrechtlich gesehen ist Datenschutz ein Aspekt des Persönlichkeitsschutzes. Das Bundesverfassungsgericht hat das Recht auf informationelle Selbstbestimmung im Volkszählungsurteil vom 15. Dezember 1983 aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz entwickelt. Das Ziel dieses Rechts ist nicht primär der Schutz von Daten, sondern die Personen zu schützen, deren Entfaltung durch Datensammlung und -nutzung bedroht wird.[39]

Der Hauptunterschied besteht darin, dass Datensicherheit sich auf den umfassenden Schutz von Daten als Ganzes konzentriert, während Datenschutz speziell auf den Schutz personenbezogener Daten abzielt und den Fokus auf die rechtmäßige und ethische Verarbeitung von Informationen, die eine Person identifizieren können, legt. Beide Ansätze sind eng miteinander verflochten und spielen eine entscheidende Rolle im Kontext einer umfassenden Informations- und IT-Sicherheitsstrategie.

5. Vorteile von Cloud-Computing

Cloud-Computing bietet dem öffentlichen Sektor eine Reihe von Vorteilen. Es ermöglicht erhebliche Kosteneinsparungen, da öffentliche Einrichtungen nur für die tatsächlich genutzten IT-Ressourcen zahlen und somit auf große Investitionen in Hardware verzichten können. Ein weiterer großer Vorteil ist die Skalierbarkeit und Flexibilität. Behörden können ihre IT-Ressourcen in Echtzeit anpassen, sie je

[39] Vgl. Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83, Rn. 1 – 215.

nach Bedarf erhöhen oder reduzieren, was besonders in Zeiten von Notfällen oder bei plötzlichen Änderungen der Anforderungen von Vorteil ist. Diese Flexibilität erlaubt es, schnell auf Veränderungen zu reagieren, ohne dass es zu Verzögerungen oder Engpässen kommt. Dies ist insbesondere in Bereichen wie dem Gesundheitswesen von entscheidender Bedeutung, wo eine schnelle Anpassungsfähigkeit wichtig sein kann.[40]

Die verbesserte Zugänglichkeit und Mobilität ist ebenfalls ein entscheidender Vorteil. Durch die Cloud können öffentliche Dienste und Daten von überall mit Internetzugang abgerufen werden. Dies fördert die Effizienz, da Beamte und Angestellte von verschiedenen Standorten aus arbeiten können. In Krisenzeiten, wie während der COVID-19-Pandemie, hat sich dies als besonders wertvoll erwiesen, da Mitarbeiter von zuhause arbeiten konnten. Die schnelle Bereitstellung und Implementierung neuer Anwendungen und Dienste wird ebenfalls erleichtert, was es dem öffentlichen Sektor ermöglicht, Projekte zügig umzusetzen und auf neue Anforderungen zu reagieren. Des Weiteren sorgt die Cloud für robuste Sicherheits- und Backup-Lösungen, die den Schutz sensibler Bürgerdaten und Verwaltungsinformationen gewährleisten. Der reduzierte Wartungsaufwand, den Cloud Computing bietet, stellt ebenfalls einen großen Vorteil dar. Da die Verantwortung für die IT-Infrastruktur beim Cloud-Anbieter liegt, können öffentliche Institutionen ihre internen Ressourcen effizienter nutzen und sich auf ihre Kernaufgaben konzentrieren. Dies bedeutet, dass weniger Zeit und Geld für die Wartung, Aktualisierung und Verwaltung von Hardware und Software aufgewendet werden müssen, was insbesondere für Behörden mit begrenztem IT-Personal von großer Bedeutung ist. Abschließend sichern die hohe Zuverlässigkeit und Verfügbarkeit von Cloud-Diensten die kontinuierliche Betriebsbereitschaft durch redundante Systeme und ermöglichen den Zugang zu neuesten Technologien, die die Weiterentwicklung und Verbesserung öffentlicher Dienstleistungen unterstützen.[41]

[40] Vgl. Hennrich, in: Heckmann (Hrsg.), Internetrecht und Digitale Gesellschaft, Band 4, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, S. 54 - 55.
[41] Vgl. Schläger, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 631, Rn.169.

6. Datenschutzrisiken und -herausforderungen

Unabhängig den Vorteilen des Cloud-Computings müssen öffentliche Institutionen bei der Nutzung von Cloud-Diensten besondere Datenschutzrisiken und Herausforderungen berücksichtigen. Diese Risiken betreffen insbesondere die Sicherheit und Vertraulichkeit der von Behörden verwalteten Daten, die besonders sensibel und schutzbedürftig sind.

6.1 Gemeinsame Nutzung gepoolter IT-Ressourcen

Eine zentrale Herausforderung im Cloud-Computing ist die gemeinsame Nutzung gepoolter IT-Ressourcen. In einem solchen Umfeld teilen sich mehrere Nutzer dieselben physischen Kapazitäten, was potenzielle Risiken hinsichtlich der Datentrennung und des Zugriffs mit sich bringt.[42] Da öffentliche Institutionen in den meisten Bereichen personenbezogene Daten verwalten, ist die Gefahr, dass diese Daten unbeabsichtigt zugänglich werden, besonders schwerwiegend. Insbesondere für Behörden, die hohe Standards in Bezug auf Datensicherheit und Datenschutz erfüllen müssen, ist es essenziell, dass starke Isolations- und Zugriffskontrollmechanismen implementiert werden. Ein Versagen dieser Mechanismen könnte nicht nur zu Datenschutzverletzungen, sondern auch zu einem Vertrauensverlust der Öffentlichkeit in staatliche Institutionen führen.

6.2 Sicherheitsmängel auf verschiedenen Ebenen

Sicherheitsmängel können sowohl auf der Ebene der Cloud-Infrastruktur als auch auf der Rechenzentrumsebene des Cloud-Anbieters auftreten. Ein unzureichendes Sicherheitskonzept kann die physische Sicherheit des Rechenzentrums gefährden, wie etwa durch unzureichende Zutrittskontrollen oder fehlende Prozessmanagement-Richtlinien. Solche Schwächen können dazu führen, dass sensible Daten in falsche Hände geraten oder ungewollt an Dritte weitergegeben werden.[43]

[42] Vgl. Jansen/Grance, NIST Special Publication 800-144, S. 11, Anlage 3.
[43] Vgl. Hennrich, Cloud-Computing nach der Datenschutz-Grundverordnung, S. 190 – 191.

6.3 Grenzüberschreitende Datenverarbeitung

Ein weiteres Risiko im Cloud-Computing ergibt sich aus der grenzüberschreitenden Datenverarbeitung. Personenbezogene Daten können in verschiedenen Ländern verarbeitet werden, deren gesetzliche Regelungen nicht den strengen Datenschutzstandards der Europäischen Union entsprechen, was zu erheblichen Compliance-Problemen führen kann. Für öffentliche Institutionen ist es besonders wichtig, sicherzustellen, dass die Verarbeitung von Daten im Einklang mit nationalen und internationalen Datenschutzgesetzen erfolgt. Ein besonderes Risiko stellt der Zugriff von ausländischen Geheimdiensten auf die Daten dar, wie es etwa durch den US-amerikanischen CLOUD Act ermöglicht wird. Der öffentliche Sektor muss sicherstellen, dass seine Daten jederzeit den strengen Anforderungen an Datensouveränität und Datenschutz genügen.[44]

6.4 Abhängigkeit von Cloud-Anbietern

Die Abhängigkeit von einem bestimmten Cloud-Anbieter kann für Behörden zu einem erheblichen Kontrollverlust führen. Wenn Behörden ihre IT-Infrastrukturen und Daten in die Cloud verlagern, geben sie die direkte Kontrolle über sensible Daten ab. Diese Daten werden auf den Servern des Cloud-Anbieters gespeichert, oft in geografisch verteilten Rechenzentren, deren genaue Standorte und Sicherheitsstandards den Behörden nicht immer transparent sind. Der Kontrollverlust erstreckt sich auch auf die Überwachung und Steuerung der Datenverarbeitung: Behörden können nur eingeschränkt nachvollziehen welche Sicherheitsmaßnahmen tatsächlich angewendet werden. Dies kann insbesondere in kritischen Bereichen problematisch sein, in denen die Einhaltung strenger Datenschutzgesetze zwingend erforderlich ist. Darüber hinaus erschwert der fehlende Einblick in die technischen und organisatorischen Prozesse des Anbieters die Gewährleistung der Datenintegrität und -vertraulichkeit, was das Risiko erhöht, dass sensible Daten in den Besitz Unbefugter gelangen und missbraucht werden.[45]

[44] Vgl. Wissenschaftliche Dienste des Deutschen Bundestages, S. 3, Anlage 5.
[45] Vgl. Jansen/Grance, NIST Special Publication 800-144, S. 12, Anlage 4.

Ein weiteres erhebliches Risiko für Behörden bei der Nutzung von Cloud-Diensten ist die Unsicherheit hinsichtlich der vollständigen Löschung von Daten. Viele Cloud-Anbieter können Daten nach Vertragsende oder auf Wunsch der Behörde möglicherweise nicht vollständig löschen. Obwohl die Daten aus dem direkten Zugriff entfernt werden, können sie in Backups, redundanten Systemen oder aufgrund technischer Einschränkungen weiterhin bestehen bleiben. Das Problem wird verschärft, wenn nach Vertragsabschluss weitere Unterauftragnehmer beauftragt werden, ohne dass die Zustimmung der Kunden explizit eingeholt wird. Zudem fehlen oft geregelte Prozesse, um mit Fällen umzugehen, in denen Kunden der Unterbeauftragung nicht zustimmen oder nachträglich widersprechen.[46] Dies stellt ein ernsthaftes Problem dar, insbesondere wenn es sich um sensible oder vertrauliche Daten handelt, die aus rechtlichen oder sicherheitsrelevanten Gründen unwiderruflich gelöscht werden müssen. Grundsätze wie Speicherbegrenzung, Löschung, Datenminimierung und Zweckbindung können dadurch verletzt werden.

6.5 Cyberattacken

Cloud-Umgebungen sind ein attraktives Ziel für Cyberattacken, wie die Verbreitung von Schadsoftware. Ein erfolgreicher Angriff kann zum Verlust von Daten oder zu massiven Betriebsstörungen führen. Die Anforderungen an sichere Verschlüsselungsverfahren sind daher besonders hoch, um den Schutz der Daten sowohl bei der Speicherung als auch während der Übertragung zu gewährleisten.

Gemäß dem Lagebericht des BSI aus dem Jahr 2023 sind insbesondere Kommunalverwaltungen, überdurchschnittlich oft von Angriffen mit Ransomware, einer Art Schadsoftware, betroffen.[47]

Als Malware („malicious software“) wird jegliche Schadsoftware bezeichnet, die sich schädigend auf Computersysteme auswirkt. Dabei kann Malware, beispielweise als Virus, Wurm oder Trojaner, den Zugriff auf Daten, Programme oder Anwendungen blockieren. Während ein Virus nur mittels einer Datei oder eines

[46] Vgl. Schläger, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 632, Rn.172.
[47] Vgl. Landtag von Baden-Württemberg, Drucksache 17 / 6100, S. 57.

Programms übertragen werden kann, verfügt ein Wurm über die Fähigkeit, sich selbstständig zu verbreiten, indem Kontaktdaten aus digitalen Adressbüchern und E-Mail-Programmen oder Netzwerkverbindungen genutzt werden. Ein Trojaner kann wiederum sowohl einen Wurm als auch einen Virus enthalten. Schadprogramme verbreiten sich häufig über E-Mail Anhänge oder manipulierte drive-by-Download Webseiten. Nutzer merken manchmal gar nicht, dass Schadsoftware auf ihrem Computer installiert wurde, da nicht alle Programme Daten manipulieren oder verschlüsseln. Manche Programme zielen darauf ab, einen illegalen Zugang zu schaffen. Zudem ist Malware oft Bestandteil weiterer Bedrohungsformen wie beispielsweise Ransomware oder Phishing.[48]

Ransomware ist eine Form von Schadsoftware, die darauf abzielt, den Zugriff auf Computersysteme oder Daten zu blockieren. Sie verschlüsselt Dateien oder sperrt den Zugriff und fordert von den Opfern Geld, um die Daten freizugeben.[49]

Unter Phishing (zusammengesetzt aus „P“ wie „Passwort“ und „fishing“, übersetzt „fischen“) versteht man einen Cyberangriff, bei dem Nutzer von Cloud-Diensten, wie Online-Speicher und E-Mail-Diensten, häufig betroffen sind. Beim Phishing versucht der Täter, geheime Identifikationsdaten des Opfers, beispielsweise Passwörter oder Zugangsdaten für Bankkonten, durch das Mitwirken des Opfers in Erfahrung zu bringen. Betroffene werden oft durch eine E-Mail aufgefordert, über einen Link, der zur scheinbaren Webseite einer Bank führt, die Zugangsdaten einzugeben. Vertrauliche Daten gelangen so in Kenntnis des Täters und dieser kann ggf. mit diesen Daten betrügerische Transaktionen, zum Beispiel eine Überweisung vom Bankkonto des Opfers, vornehmen.[50]

[48] Vgl. Wollinger/Schulze, Handbuch Cybersecurity für die öffentliche Verwaltung, S. 42 – 46.
[49] Vgl. Wollinger/Schulze, Handbuch Cybersecurity für die öffentliche Verwaltung, S. 46 – 48.
[50] Vgl. Wollinger/Schulze, Handbuch Cybersecurity für die öffentliche Verwaltung, S. 52 – 53.

7. Technische und organisatorische Maßnahmen in der Cloud

Um Datenschutzrisiken wie Cyberangriffen entgegenzuwirken, sind bei den verschiedenen Cloud-Modellen und Services bestimmte technische und organisatorische Maßnahmen (TOM) zu beachten. Das Ziel besteht darin, TOM bereits in die Technologie zu integrieren, wobei diese Maßnahmen zu jedem Zeitpunkt der Datenverarbeitung eingesetzt werden können.

Gemäß Art. 32 Abs. 1 der DSGVO sind geeignete TOM erforderlich, die darauf abzielen, einen unzulässigen Umgang mit personenbezogenen Daten zu verhindern. Dies dient dem Schutz der informationellen Selbstbestimmung, indem sichergestellt wird, dass Daten vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung geschützt sind.

Zu den spezifischen Maßnahmen gemäß Artikel 32 Abs. 1 der DSGVO gehören die Pseudonymisierung und Verschlüsselung personenbezogener Daten sowie die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Zudem beinhalten sie Mechanismen zur Wiederherstellung der Datenverfügbarkeit und des Zugangs im Fall von physischen oder technischen Zwischenfällen, sowie ein regelmäßiges Evaluierungsverfahren der Sicherheitsmaßnahmen.

7.1 Technische Maßnahmen

Technische und organisatorische Maßnahmen sind nach Art. 32 DSGVO an den Stand der Technik anzupassen. Diese Verpflichtung bedeutet, dass bei der Planung und Umsetzung solcher Maßnahmen aktuelle und bewährte Standards sowie Best-Practice-Ansätze genutzt werden müssen. Die Wirksamkeit der bereits umgesetzten Maßnahmen sollte regelmäßig überprüft und veraltete Maßnahmen durch modernere Mechanismen ersetzt werden. Die DSGVO legt jedoch nicht fest, was genau als Stand der Technik gilt und wer dies definiert. Im Folgenden werden einige technische Maßnahmen erläutert, die dem jetzigen Stand der Technik entsprechen.[51]

[51] Vgl. Schläger, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 545.

7.1.1 Pseudonymisierung

Die Pseudonymisierung ist ein zentrales Mittel, um die Vertraulichkeit und Integrität von Daten zu gewährleisten und wird daher als eine der wenigen Sicherheitsmaßnahmen explizit in Art. 32 der DSGVO genannt. Pseudonymisierung bedeutet, personenbezogene Daten so zu verarbeiten, dass sie ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können. Diese zusätzlichen Informationen werden separat aufbewahrt und durch weitere geeignete TOM geschützt.[52] Nach dem allgemeinen Sprachverständnis ist unter „Pseudonym“ ein erfundener Deckname zu verstehen, der die wahre Identität einer Person verschleiert.[53] Die ENISA hat einen Leitfaden zu Pseudonymisierungstechniken entwickelt, in dem mehrere Methoden aufgezeigt werden. Unter anderem enthält der Leitfaden die Pseudonymisierungstechnik, bei der Identifikatoren durch eine fortlaufende Nummer ersetzt werden können.[54] Behörden könnten vor Übertragung der Daten in die Cloud sensible Daten wie Name, Adresse oder Bankdaten durch alphanumerische Codes ersetzen, wobei die Zuordnungsdatei in einer getrennten, geschützten Datenbank am besten auf behördeninternen Rechnern gespeichert wird. So kann die Behörde Daten in der Cloud verarbeiten, ohne die Privatsphäre der Bürger zu gefährden. Mithilfe von Softwarelösungen kann dieser Prozess automatisiert und effizient gestaltet werden.

Das Verwenden von Pseudonymen kann nicht nur der Vertraulichkeit von Daten dienen, sondern auch der Datenminimierung. Durch eine Pseudonymisierung bleiben weniger identifizierbare Daten verfügbar und beschränken die Datenverarbeitung in der Cloud auf das Notwendigste.

7.1.2 Verschlüsselung

Auch die Verschlüsselung ist eine wesentliche Maßnahme, die ausdrücklich in Artikel 32 der DSGVO genannt wird. Unter Verschlüsselung ist ein Vorgang zu verstehen, bei dem eine klar lesbare Information beispielsweise durch eine Ersetzungstabelle eines kryptographischen oder mathematischen Verfahrens ersetzt bzw.

[52] Vgl. Art. 4 Nr. 5 DSGVO; § 46 Nr. 5 BDSG.
[53] Vgl. Gola, in: Gola/Heckmann (Hrsg.), DS-GVO, Kommentar, Art. 4, Rn. 46.
[54] Vgl. ENISA, Data Pseudonymisation: Advanced Techniques and Use Cases, S. 12.

verschleiert wird. Dabei wird grundsätzlich zwischen Transportverschlüsselung, Ende-zu-Ende-Verschlüsselung und Speicherverschlüsselung unterschieden. Zudem gibt es eine Vielzahl von Verschlüsselungsalgorithmen mit unterschiedlichen Funktionsweisen, wobei zwischen symmetrischen und asymmetrischen Verfahren unterschieden wird.[55]

Symmetrische Verschlüsselungsverfahren nutzen denselben Schlüssel sowohl für das Ver- als auch für das Entschlüsseln von Daten, wobei die Entschlüsselung eine Umkehrung der Verschlüsselung darstellt. Ein einfaches Beispiel hierfür ist die Caesar-Verschlüsselung, bei der die Buchstaben eines Textes um eine bestimmte Anzahl im Alphabet verschoben werden. Moderne symmetrische Verfahren arbeiten zwar nicht mehr direkt mit Buchstaben, basieren aber auf einem ähnlichen Prinzip: Ein Schlüssel wird verwendet, um Daten zu verschlüsseln, und derselbe Schlüssel wird in umgekehrter Form für die Entschlüsselung genutzt. Da das Verschlüsselungsverfahren bekannt ist, ist es bei der symmetrischen Verschlüsselung entscheidend, den Schlüssel streng vertraulich zu halten.[56] Zudem muss dieser erst zwischen Absender und Empfänger geheim ausgetaucht werden. Durch den Diffie-Hellman-Schlüsselaustausch kann dieses Problem einfach gelöst werden, indem der geheime Schlüssel gemeinschaftlich von den Kommunikationspartnern berechnet wird.[57] Eine einfache Anwendung symmetrischer Verschlüsselung findet sich beispielsweise bei Packprogrammen wie ZIP (gezippte Datei), welche verschlüsselte Dateiarchive erstellen, die nur mit dem entsprechenden Passwortschlüssel zugänglich sind. Wenn verschlüsselte ZIP-Dateien beispielsweise per E-Mail versendet werden, können Dritte, die keinen Zugriff auf den Schlüssel haben, nicht auf den Inhalt der Datei zugreifen. Diese Methode stellt sicher, dass selbst wenn die E-Mail auf dem Weg abgefangen wird, der Inhalt der ZIP-Datei nicht entschlüsselt werden kann.[58] Als ein internationaler Standard für die symmetrische Verschlüsselung hat

[55] Vgl. Meyer/Schmidt, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 618, Rn. 108.
[56] Vgl. Rahden, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 619, Rn. 110 - 113.
[57] Vgl. Rahden, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 621, Rn. 119 - 120.
[58] Vgl. Martini, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, Art. 32 Sicherheit der Verarbeitung, Rn. 34a.

das NIST den Advanced Encryption Standard (AES) eingeführt. [59] AES ist ein symmetrischer Verschlüsselungsalgorithmus, der als offizieller Verschlüsselungsstandard etabliert ist. Es gibt verschiedene Verschlüsselungsgrößen (128, 192 und 256 Bit), wobei die Stärke der Verschlüsselung mit der Schlüsselgröße zunimmt.[60] AES wird in zahlreichen Anwendungen und Protokollen weltweit genutzt, z. B. in Virtual Private Networks und bei der Festplattenverschlüsselung (im Ruhezustand). Die Technische Richtlinie TR-02102-1 des BSI empfiehlt ausdrücklich, AES, bevorzugt mit einem sicheren Betriebsmodus, beispielsweise XTS-AES für die Festplattenverschlüsselung, zu verwenden.[61]

Anders ist es bei der asymmetrischen Verschlüsselung, bei der zwei verschiedene Schlüssel genutzt werden: einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln. Der Vorteil dieser Methode ist, dass vertrauliche Nachrichten verschlüsselt werden können, ohne dass zuvor ein geheimer Schlüssel ausgetauscht werden muss. Da diese asymmetrischen Verfahren auf komplexen mathematischen Berechnungen basieren, nimmt die Ver- oder Entschlüsselung deutlich mehr Rechenleistung als die symmetrische Verschlüsselung in Anspruch und ist bei großen Datenmengen eher weniger effizient.[62] Das BSI empfiehlt unter anderem als asymmetrische Verschlüsselung das RSA-Verfahren, welches nach seinen Erfindern Rivest, Shamir und Adleman benannt wurde und beispielsweise bei der Authentifizierung von Dokumenten eingesetzt wird. Die Schlüssellänge sollte mindestens 3.000 Bits betragen, da es laut dem BSI ab dieser Größe praktisch unmöglich ist, den Schlüssel zu entschlüsseln.[63]

Die Transportverschlüsselung schützt Daten während der Übertragung über Netzwerke, indem sie den Datenverkehr zwischen Sender und Empfänger verschlüsselt, wodurch ein sicherer Kanal entsteht. Ein bekanntes Protokoll hierfür ist TLS (Transport Layer Security), welches häufig für die sichere Übertragung von Webseiten genutzt wird und an der URL (Uniform Resource Locator) „https://“ zu

[59] Vgl. NIST, FIPS Publication 197, S. 1, Anlage 6.
[60] Vgl. BSI, Technische Richtlinie TR-02102-1, S. 21.
[61] Vgl. BSI, Technische Richtlinie TR-02102-1, S. 25.
[62] Vgl. Rahden, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 619-621, Rn. 114 - 122.
[63] Vgl. BSI, Technische Richtlinie TR-02102-1, S. 33 – 35, Anlage 7.

erkennen ist. Eine weitere Möglichkeit für einen sicheren Kanal stellt der Remote-Zugang über ein abgesichertes Virtual Private Network (VPN) dar.[64]

Ein konventionelles VPN erstellt ein sicheres, virtuelles Netzwerk über ein bestehendes Kommunikationsnetz wie das Internet. Es ermöglicht, dass Mitarbeiter einer Behörde von außen (z. B. von zu Hause) Zugriff auf das Behördennetzwerk haben, als wären sie direkt vor Ort. Die Verbindung wird durch ein VPN-Gateway hergestellt, das das Heimnetz und das Internet als eine Art „Verlängerungskabel“ betrachtet, um den Zugriff auf das Netz der Behörde zu ermöglichen.[65]

Die Ende-zu-Ende-Verschlüsselung hingegen ermöglicht die verschlüsselte Kommunikation zwischen Absender und Empfänger. Dienstanbieter, die eine solche Plattform zum Austausch betreiben, haben keinen unverschlüsselten Zugriff auf die ausgetauschten Daten. Nur Absender und Empfänger können die Nachricht unverschlüsselt lesen. Allerdings bleiben bei der Ende-zu-Ende-Verschlüsselung die Metadaten wie z. B. Sender, Empfänger, Zeitstempel und bei E-Mails der Betreff lesbar, auch gegenüber dem Dienstanbieter. Um auch die Metadaten zu verschlüsseln, sollte eine Transportverschlüsselung mit einer Ende-zu-Ende-Verschlüsselung kombiniert werden.[66]

Diese verschiedenen Verschlüsselungsmethoden tragen vor allem dem Grundsatz der Vertraulichkeit bei, da die Verschlüsselung vor unbefugtem Zugriff schützt und sicherstellt, dass nur berechtigte Personen mit den entsprechenden Schlüsseln auf die Daten zugreifen können. Es ist allerdings wichtig zu beachten, dass selbst nach der Verschlüsselung der personenbezogenen Daten weiterhin personenbezogene Daten vorliegen. Verschlüsselte Merkmale können theoretisch entschlüsselt werden und ggf. eine Person identifizieren.

---

[64] Vgl. Schläger in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 633, Rn. 178.
[65] Vgl. Schmidt/Pruß,in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 3 Technische Grundlagen des Internets Rn. 319.
[66] Vgl. Rahden, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 625-627, Rn. 142 - 151.

7.1.3 Anonymisierung

Unter Anonymisierung ist das Verändern personenbezogener Daten zu verstehen, sodass Personen nicht mehr identifiziert werden können. In der DSGVO wird die Anonymisierung nicht definiert, aber im Erwägungsgrund 26 näher beschrieben. Die Grundsätze des Datenschutzes sind auf anonyme Daten nicht mehr anwendbar. Um Daten zu anonymisieren, wird der Personenbezug gelöscht. Datensätze bleiben erhalten, lassen aber keine Zuordnung zu einer bestimmten oder bestimmbaren Person zu. [67] Da der Personenbezug von Daten im öffentlichen Sektor notwendig ist, ist die Anonymisierung vor allem für die Erstellung von Statistiken geeignet, bei denen der Personenbezug nicht erforderlich ist.

Ob ein Personenbezug und damit personenbezogene Daten vorliegen, lässt sich durch zwei unterschiedliche Betrachtungsweisen feststellen. Betrachtet man Daten durch den absoluten Ansatz, genügt bereits die objektive Möglichkeit, dass irgendjemand eine Person potenziell anhand eines Datums identifizieren könnte. In der Ära von Big Data[68] und der fortgeschrittenen technischen Möglichkeiten, Daten zu verknüpfen und Anonymisierungen rückgängig zu machen, erweitert dieser Ansatz den Anwendungsbereich des Datenschutzrechts nahezu unbegrenzt. Demgegenüber betrachtet der subjektive Ansatz die Möglichkeit, Zusatzwissen lediglich aus der Perspektive des jeweiligen Verantwortlichen heranzuziehen. Wenn die verarbeitende Stelle durch ihr Wissen oder durch die Möglichkeit, dieses Wissen mit einem angemessenen Aufwand an Arbeitskraft, Kosten und Zeit zu erweitern (z. B. durch Befragungen oder Berechnungen), in der Lage ist, Einzelangaben einer bestimmten Person zuzuordnen, dann handelt es sich um personenbezogene Daten. Wenn die verarbeitende Stelle jedoch nicht in der Lage ist, diese Zuordnung vorzunehmen, so ist der Betroffene nicht identifizierbar und die Einzelangaben stellen subjektiv betrachtet keine personenbezogenen Daten dar.[69]

---

[67] Vgl. Ernst, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, Art. 4 Begriffsbestimmungen, Rn. 48-51.

[68] Big Data bezeichnet große, komplexe und schnell wachsende Datenmengen und wird durch die „drei Vs“ charakterisiert: Volume (Datenmenge), Velocity (Geschwindigkeit) und Variety (Vielfalt). Vgl. Weber in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S. 127 - 128, Rn. 5.

[69] Vgl. Hartung/Storm, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 334 - 337, Rn. 25 - 28.

7.1.4 Zugangs- und Zugriffsmanagement

Zusätzlich zur Verschlüsselung oder Pseudonymisierung von Daten sind Zugangs- und Zugriffskontrollen zur Gewährleistung von Integrität und Vertraulichkeit dienlich. Die Zugangskontrolle soll verhindern, dass Unbefugte auf Datenverarbeitungssysteme zugreifen. Das bedeutet, dass sie nicht auf IT-Systeme und deren Anwendungen zugreifen können, obwohl sie eigentlich für autorisierte Nutzer gedacht sind. Um die Zugangskontrolle umzusetzen, können verschiedene Maßnahmen ergriffen werden, wie zum Beispiel Berechtigungsprüfungen, strenge Passwortregeln und die Nutzung von Firewalls.[70]

Eine Firewall ist ein softwarebasiertes Sicherheitssystem, das Netzwerke oder Computer vor unerwünschten Zugriffen schützt, indem es den Datenverkehr nach Absender, Ziel und genutzten Diensten kontrolliert. Sie überwacht kontinuierlich den Netzwerkverkehr und entscheidet anhand festgelegter Regeln, welche Datenpakete zugelassen oder blockiert werden, um unbefugte Zugriffe zu verhindern. Firewalls gibt es in zwei Haupttypen: Personal Firewalls, die direkt auf dem zu schützenden Gerät installiert sind, und externe Firewalls, die auf separaten Geräten arbeiten und den Datenverkehr zwischen verschiedenen Netzwerken regeln. Während Firewalls sehr effektiv darin sind, den Zugang zu kontrollieren und unerlaubte Verbindungen abzuwehren, stoßen sie an ihre Grenzen, wenn es darum geht, autorisierte, aber bösartige Aktivitäten innerhalb erlaubter Verbindungen zu erkennen.[71]

Hier kommen Intrusion Detection and Prevention Systems (IDPS) ins Spiel, die eine ergänzende Schutzschicht bieten. Ein IDPS überwacht den Netzwerkverkehr nicht nur auf erlaubte oder verbotene Verbindungen, sondern analysiert auch den Inhalt dieser Verbindungen und das Verhalten im Netzwerk. Dadurch kann es verdächtige Aktivitäten aufdecken, die eine Firewall möglicherweise übersehen

[70] Vgl. Hennrich, in: Heckmann (Hrsg.), Internetrecht und Digitale Gesellschaft, Band 4, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, S. 209.
[71] Vgl. Schmidt/Pruß,in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 3 Technische Grundlagen des Internets Rn. 283.

würde. Wenn das IDPS eine Bedrohung erkennt (detect), kann es automatisch Maßnahmen ergreifen, wie das Blockieren des schädlichen Datenverkehrs oder das Isolieren eines betroffenen Systems, um den Angriff zu verhindern (prevent).[72]

Zusammen bieten Firewalls und IDPS eine umfassendere Sicherheitslösung: Die Firewall kontrolliert den Zugriff auf das Netzwerk, während das IDPS dafür sorgt, dass auch innerhalb erlaubter Verbindungen keine unbemerkten Angriffe stattfinden. Ergänzt werden diese Systeme durch moderne Ansätze wie Security as a Service (SECaaS), die es ermöglichen, diese und andere Sicherheitsdienste flexibel in der Cloud zu nutzen. SECaaS umfasst neben Firewalls und IDPS auch andere wichtige Sicherheitsmaßnahmen wie Verschlüsselung oder Identitäts- und Zugriffsmanagement. Diese Dienste können nach Bedarf angepasst werden, um den spezifischen Anforderungen gerecht zu werden und bieten dadurch eine umfassende und flexible Sicherheitslösung.[73]

Des Weiteren sollten mehrere zentrale Aspekte beim Passwortschutz beachtet werden. Das NIST empfiehlt Passwörter mit mindestens zwölf Zeichen, da längere Passwörter schwerer zu knacken sind. Zudem sollten Passwörter nicht in regelmäßigen Abständen geändert werden, sondern nur, wenn es Anzeichen einer Sicherheitslücke gibt. Außerdem sollten keine Passwörter wiederverwendet werden.[74]

Im Gegensatz zur Zugangskontrolle bezieht sich die Zugriffskontrolle auf den Zugriff von grundsätzlich Berechtigten außerhalb ihrer zugewiesenen Berechtigung. Die Zugriffskontrolle stellt sicher, dass nur erlaubte Nutzer auf bestimmte Daten zugreifen können. Außerdem soll sie verhindern, dass personenbezogene Daten während ihrer Verarbeitung, Nutzung und Speicherung unbefugt eingesehen, kopiert, verändert oder gelöscht werden können. Diese Kontrolle erfolgt hauptsächlich durch Rechteverwaltungen, die Zugriffsrechte und -berechtigungen über

[72] Vgl. Schmidt/Pruß,in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 3 Technische Grundlagen des Internets Rn. 288.
[73] Vgl. Hennrich in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S. 459, Rn. 13.
[74] Vgl. NIST, Special Publication 800-63B, S. 13 – 14, Anlage 8.

Betriebssysteme und Verzeichnisdienste steuern, sowie durch Maßnahmen zur Authentisierung, Authentifizierung und Autorisierung.[75]

Unter Authentisierung versteht man den Vorgang, bei dem ein Nutzer einem Kommunikationspartner seine Identität nachweist. Es findet eine Identifizierung statt, bei der Berechtigungsnachweise übermittelt werden, beispielsweise durch Eingeben eines Nutzernamens. Der anschließende Vorgang des Überprüfens dieser Information heißt Authentifizierung. Die Authentifizierung stellt sicher, dass die angegebene Identität eines Nutzers korrekt ist und autorisiert werden kann. Bei der Autorisierung werden einem Nutzer die zugewiesenen Rechte eingeräumt.[76]

Im Zuge der Authentifizierung können drei verschiedene Faktoren abgefragt werden. Der erste Faktor basiert auf dem Wissen der Person (something you know), beispielsweise einer PIN oder einem Nutzernamen mit Passwort. Der zweite Faktor beinhaltet alle Attribute, die unmittelbar Teil der Person sind, also biologische Eigenschaften der Person (something you are), beispielsweise Fingerabdruck oder Iris des Auges. Der dritte Faktor basiert auf Gegenständen, die sich im Besitz einer Person befinden (something you have), beispielsweise einem Security-Token. Mehr Sicherheit gewährleistet eine Kombination dieser Faktoren, eine sog. Mehr-Faktor-Authentifizierung, die aber kein Muss ist.[77]

Zudem muss die Verarbeitung von Daten auf Dauer sichergestellt werden. Das bedeutet, dass Systeme und Dienste auch bei möglichen Störungen oder bei erhöhter Belastung zuverlässig funktionieren müssen. Die Anwendung muss weiterhin die geforderte Sicherheit gewähren und die Daten bei einem physischen oder technischen Zwischenfall wieder verfügbar machen können. Regelmäßige Backups zur Sicherung der Daten sind hierbei unerlässlich. Bei einem Backup wird der aktuelle Datenbestand in einer Sicherheitskopie dupliziert und kann im Falle eines Datenverlusts den Stand wiederherstellen. Es ist jedoch wichtig, dass auch Backups

[75] Vgl. Hennrich, in: Heckmann (Hrsg.), Internetrecht und Digitale Gesellschaft, Band 4, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, S. 209.
[76] Vgl. Borges/Werner, Identitätsmanagement im Cloud Computing, S. 34 – 37.
[77] Vgl. Borges/Werner, Identitätsmanagement im Cloud Computing, S. 36 – 50.

regelmäßig überprüft und veraltete oder nicht mehr benötigte Daten gelöscht werden, um sicherzustellen, dass der Datenschutz gewahrt bleibt und keine unnötigen Datenkopien bestehen bleiben.[78]

Des Weiteren ist es entscheidend, dass Systeme in der dynamischen Welt des Cloud-Computings kontinuierlich aktualisiert werden. Cloud-Umgebungen sind komplex und unterliegen ständigen Veränderungen, sei es durch neue Sicherheitsbedrohungen, technologische Fortschritte oder erweiterte Funktionsanforderungen. Regelmäßige Updates sind essenziell, um Sicherheitslücken zu schließen, die durch neue Bedrohungen entstehen können und um sicherzustellen, dass die Systeme den aktuellen Standards und gesetzlichen Anforderungen entsprechen. Ohne eine konsequente Aktualisierung besteht die Gefahr, dass Systeme veralten, Sicherheitsrisiken entstehen und die Leistungsfähigkeit sowie Zuverlässigkeit der Cloud-Dienste beeinträchtigt werden.[79]

7.1.5 Löschen von Daten aus dem Cloud-Speicher

Im Cloud-Computing ist die sichere Löschung digitaler Daten unerlässlich, um sowohl Datenschutz als auch die Wiederverwendbarkeit von Speichermedien zu gewährleisten. Anstatt Datenträger physisch zu zerstören, was endgültig und nicht nachhaltig ist, kann eine digitale Löschung erfolgen, die es ermöglicht die Datenträger weiter zu nutzen. Dabei ist im Vorfeld beim Cloud-Anbieter sicherzustellen, dass die gelöschten Daten nicht wiederhergestellt werden können.

Beim herkömmlichen Löschen über das Betriebssystem werden die Daten auf einem Speichermedium nicht tatsächlich entfernt, sondern die entsprechenden Speicherbereiche lediglich als frei markiert. Die Daten bleiben so lange auf dem Medium, bis diese Bereiche mit neuen Daten überschrieben werden. Dies birgt das Risiko, dass die ursprünglichen Daten wiederhergestellt werden können, insbesondere bei magnetischen Speichermedien wie Hard Disk Drives (HDDs). Hier können

[78] Vgl. Meyer/Schmidt, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 609, Rn. 71.
[79] Vgl. Klein-Hennig, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 649, Rn. 226.

die magnetischen Unterschiede zwischen den einzelnen Speicherbereichen ausgelesen werden, um die gelöschten Daten zu rekonstruieren. Um solche Wiederherstellungen zu verhindern, empfiehlt es sich, die Speichermedien mehrfach mit zufällig generierten Datenmustern zu überschreiben. Durch mindestens siebenfache Überschreibung kann das Risiko einer Datenrekonstruktion erheblich reduziert werden.[80] Eine solche Vorgehensweise ist in der Praxis schwer umzusetzen, da es im laufenden Betrieb nicht möglich ist, alle Daten ständig siebenfach zu überschreiben.

Bei modernen Speichern wie Solid State Disks (SSDs), die zunehmend im Cloud-Computing zum Einsatz kommen, stellt das sichere Löschen eine besondere Herausforderung dar. SSDs verwenden Speicherchips, bei denen jeder Schreibvorgang zu einer leichten Abnutzung führt. Um eine gleichmäßige Abnutzung zu gewährleisten, verschieben eingebaute Controller die Daten regelmäßig auf weniger beanspruchte Speicher-zellen. Diese Technik, die als „Wear-Leveling“ bezeichnet wird, erschwert es sicherzustellen, dass alle Bereiche einer SSD überschrieben werden, da die Daten physisch auf dem Speichermedium wandern können. Um dieses Problem zu umgehen, bieten viele SSD-Hersteller spezielle interne Löschfunktionen wie „ATA Secure Erase“ an. Diese Funktion ermöglicht es, den Controller zu umgehen und die Daten direkt auf den Speicherchips zu löschen, wodurch sichergestellt wird, dass die gesamte SSD von den Daten bereinigt wird. Diese Methode gilt als eine der zuverlässigsten, um die vollständige Löschung aller Daten auf SSDs zu gewährleisten.[81]

Es ist ersichtlich, dass das sichere Löschen von Daten im Cloud-Computing eine sorgfältige Vorgehensweise erfordert, die von der Art des Speichermediums abhängt. Während bei HDDs eine mehrfache Überschreibung der Speicherbereiche ausreicht, erfordert das Löschen von Daten auf SSDs den Einsatz spezialisierter Tools und Methoden, um die vollständige Datenvernichtung sicherzustellen. Solche Methoden sollte auch ein potenzieller Cloud-Dienstleister anbieten, da nur so

[80] Vgl. Meyer/Schmidt, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 615 - 617, Rn. 97 - 100.
[81] Vgl. Meyer/Schmidt, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 617, Rn. 101 - 104.

das Betroffenenrecht auf Löschung und die Grundsätze des Datenschutzes eingehalten werden können.

7.1.6 Checkliste für technische Maßnahmen

Als praxisnahe Hilfestellung folgt nun die Checkliste für technische Sicherheitsmaßnahmen, die in der Praxis als Unterstützung bei der Entscheidung über eine Auslagerung der Daten in die Cloud eingesetzt werden kann.

Datenverschlüsselung

- ☐ Die gespeicherten Daten werden im Ruhezustand verschlüsselt.
- ☐ Daten werden während der Übertragung in die Cloud verschlüsselt.
- ☐ Es werden aktuelle und bewährte Verschlüsselungsstandards, wie AES für ruhende Daten und TLS während des Datentransfers eingesetzt.
- ☐ Ein VPN wird verwendet, um sichere Verbindungen über das Internet herzustellen.

Pseudonymisierung

- ☐ Es werden vor der Datenübertragung in die Cloud Verfahren zur Pseudonymisierung durchgeführt.

Anonymisierung

- ☐ Es werden vor Datenübertragung in die Cloud Verfahren zur Anonymisierung, die eine Identifizierung von Einzelpersonen vollständig ausschließen, durchgeführt. (Statistiken)

Zugangs- und Zugriffsmanagement

- ☐ Zugangskontrollen sind implementiert, um unbefugten Zugang auf Systeme und Daten zu verhindern.
- ☐ Zugriffskontrollen sind implementiert, um unbefugten Zugriff auf Systeme und Daten zu verhindern.
- ☐ Mehr-Faktor-Authentifizierung wird zur Sicherung der Benutzerkonten verwendet.

Datensicherung- und Wiederherstellung

☐ Es werden regelmäßig Daten-Backups erstellt und gesichert.

☐ Die Backups sind verschlüsselt und sicher gespeichert.

Datensicherheit

☐ Es werden alle Systeme und Anwendungen regelmäßig aktualisiert, um Sicherheitslücken zu schließen.

☐ Die aktuelle Software entspricht den Sicherheitsstandards.

☐ Systeme zur Erkennung und Verhinderung von Angriffen auf die Cloud-Infrastruktur sind implementiert.

☐ Es wird sichergestellt, dass Daten vollständig und sicher gelöscht werden können.

7.2 Organisatorische Maßnahmen in der Cloud

Organisatorische Maßnahmen im Datenschutz umfassen sämtliche nichttechnische Aspekte, die darauf abzielen, den Schutz personenbezogener Daten innerhalb einer Organisation sicherzustellen. Sie ergänzen die technischen Sicherheitsmaßnahmen und tragen dazu bei, ein umfassendes Datenschutzmanagement zu etablieren, das den Anforderungen der geltenden Datenschutzgesetze und -bestimmungen gerecht wird.

7.2.1 Allgemeine organisatorische Maßnahmen

Zu diesen organisatorischen Maßnahmen gehört zunächst die Ernennung eines Datenschutzbeauftragten. Für Behörden und Auftragsverarbeiter ist gemäß Art. 37 Abs. 1 lit. a DSGVO die Bestellung eines Datenschutzbeauftragten vorgeschrieben. Diese Person ist für die Überwachung der Einhaltung der Datenschutzvorschriften in der Organisation verantwortlich und dient als Ansprechpartner für Datenschutzfragen.

Die Bestellung eines Datenschutzbeauftragten ist für Behörden nicht nur eine gesetzliche Verpflichtung, sondern auch ein entscheidender Faktor zur Gewährleistung der Einhaltung aller datenschutzrechtlichen Vorgaben. Angesichts der

umfangreichen Verarbeitung personenbezogener Daten in öffentlichen Stellen ist es unerlässlich, dass die Behörde über einen Experten verfügt, der die spezifischen Anforderungen der DSGVO kennt und umsetzt. Daher ist es von zentraler Bedeutung, den Datenschutzbeauftragten in die Auswahl eines Cloud-Anbieters und in die Vertragsgestaltung mit einzubeziehen. Seine Expertise hilft sicherzustellen, dass alle datenschutzrechtlichen Anforderungen berücksichtigt werden, insbesondere im Hinblick auf Datensicherheit, Datenverarbeitung und die Rechte der betroffenen Personen. Indem er frühzeitig in diesen Prozess eingebunden wird, können potenzielle Risiken besser identifiziert und rechtliche Fallstricke vermieden werden, was zur rechtskonformen und sicheren Nutzung von Cloud-Diensten beiträgt. In der Praxis kann die Bedeutung der Einbindung des Datenschutzbeauftragten in solche Entscheidungen leicht unterschätzt werden. Cloud-Dienstanbieter werben mit hoher Sicherheit ihrer Systeme, wodurch sich potenzielle Kunden täuschen lassen, da ihnen oft nicht bewusst ist, wie umfangreich der Datenschutz in solchen Umgebungen ist und wie weitreichend die Risiken sein können.

Zudem muss die Entwicklung und Umsetzung von Datenschutzrichtlinien und -verfahren sichergestellt sein. Durch solche Richtlinien und Verfahren soll gewährleistet werden, dass Datenschutzbelange bei allen Aktivitäten berücksichtigt werden. Sie regeln die Verarbeitung personenbezogener Daten in der Behörde und legen fest, wie Daten gesammelt, verwendet, weitergegeben und gelöscht werden dürfen, um sicherzustellen, dass sie in Übereinstimmung mit den geltenden Datenschutzgesetzen und -bestimmungen behandelt werden.[82]

Besonders wichtig ist es, dieses Knowhow an die Angestellten und Beamten der Behörde durch Schulungen und Sensibilisierung weiterzugeben. Es können Informationsveranstaltungen durchgeführt werden oder E-Learnings erstellt werden, die die Mitarbeiter über Datenschutzrichtlinien, Datenschutzbestimmungen und die Bedeutung des Schutzes personenbezogener Daten in der Cloud aufklären. Dies trägt dazu bei, das Bewusstsein für Datenschutz zu erhöhen und sicherzustellen,

[82] Vgl. Thode, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 44, Rn. 147.

dass die Mitarbeiter die richtigen Verhaltensweisen im Umgang mit sensiblen Daten kennen und befolgen.[83]

Des Weiteren ist der Datenschutzbeauftragte am Risikomanagement, einschließlich der Datenschutzfolgenabschätzung (DSFA) gemäß Art. 35 DSGVO beteiligt. Eine DSFA ist erforderlich, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Dies kann die Behörde beispielsweise bei der Verarbeitung von Gesundheitsdaten oder der Überwachung öffentlicher Bereiche betreffen. Eine genaue Auflistung, für welche Verarbeitungsvorgänge eine solche DSFA durchzuführen ist, kann der Liste des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) entnommen werden.[84] Die DSFA ist ein strukturiertes Verfahren zur Bewertung der Auswirkungen geplanter Datenverarbeitungsvorgänge auf den Schutz personenbezogener Daten. Der Prozess besteht aus mehreren Schritten, die dabei helfen, potenzielle Risiken frühzeitig zu erkennen und geeignete Schutzmaßnahmen zu entwickeln. Auch wenn eine DSFA nicht bei jeder Verarbeitung gesetzlich zwingend vorgeschrieben ist, empfiehlt es sich dennoch, besonders in Anbetracht der Nutzung von Cloud-Diensten, eine solche durchzuführen. Öffentliche Institutionen können durch eine gründliche DSFA sicherstellen, dass alle datenschutzrelevanten Aspekte angemessen berücksichtigt werden, was besonders bei der Wahrung der Grundsätze der DSGVO von Bedeutung ist. Eine DSFA enthält gemäß Art. 35 Absatz 7 DSGVO Folgendes:

- Beschreibung der geplanten Verarbeitung (Art. 35 Abs. 7 lit. a DSGVO)

  Der Verantwortliche muss die geplante Verarbeitung detailliert beschreiben. In dieser Beschreibung sollte dargelegt werden, welche Arten von personenbezogenen Daten verarbeitet werden, in welchem Umfang und zu welchem Zweck die Verarbeitung erfolgt sowie unter welchen Umständen dies geschieht, einschließlich der eingesetzten Cloud-Infrastruktur und beteiligten Dienstleister.

[83] Vgl. Herbst, in: Seckelmann (Hrsg.) Digitalisierte Verwaltung Vernetztes E-Government, S 396, Rn. 37.; Art. 39 DSGVO

[84] BfDI, Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, (o. S.), Anlage 9.

- Notwendigkeit und Verhältnismäßigkeit der Verarbeitung (Art. 35 Abs. 7 lit. b DSGVO)

  Die DSFA prüft auch die rechtliche Grundlage der Verarbeitung und stellt sicher, dass nur die für den Zweck erforderlichen Daten verarbeitet werden. Dadurch werden die Grundsätze der Rechtmäßigkeit und Datenminimierung geprüft.

- Bewertung der Risiken für die Betroffenen (Art. 35 Abs. 7 lit. c DSGVO)

  Risiken für Betroffene müssen analysiert werden, um sicherzustellen, dass die Daten auch in einer externen Umgebung sicher sind. Da die physische Kontrolle über die Daten beim Cloud-Anbieter liegt, müssen Maßnahmen definiert werden, die das Risiko von Datenverlusten oder -missbrauch reduzieren.

- Maßnahmen zur Bewältigung der Risiken (Art. 35 Abs. 7 lit. d DSGVO)

  Um die identifizierten Risiken zu minimieren, werden technische und organisatorische Maßnahmen definiert, wie z. B. die Verschlüsselung der Daten, Zugangskontrollen und regelmäßige Sicherheitsüberprüfungen durch den Cloud-Anbieter. Diese Maßnahmen schützen die Integrität und Vertraulichkeit der Daten. Außerdem sollte dokumentiert werden, wie die Einhaltung dieser Maßnahmen durch den Cloud-Anbieter regelmäßig überwacht wird, um sicherzustellen, dass die Sicherheitsanforderungen erfüllt bleiben.

- Dokumentation und Entscheidung

  Die Ergebnisse der DSFA werden in einem Bericht dokumentiert und dienen als Nachweis dafür, dass alle Risiken im Zusammenhang mit der Cloud-Nutzung bewertet und Maßnahmen zur Minimierung getroffen wurden.

Da Cloud-Dienste dynamisch und oft in ständigem Wandel sind, muss die DSFA regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass die Integrität, Vertraulichkeit und Sicherheit der Daten dauerhaft gewährleistet sind.[85]

[85] Vgl. DSK, Kurzpapier Nr. 5, S. 2, Anlage 10.

Die Dokumentation und Nachweisbarkeit sind nicht nur bei der DSFA von zentraler Bedeutung, sondern dienen auch dem Grundsatz der Rechenschaftspflicht. Die lückenlose Dokumentation aller Datenschutzmaßnahmen, -richtlinien und -verfahren ist unerlässlich, um die Einhaltung der Datenschutzvorschriften nachzuweisen und bei Überprüfungen durch Aufsichtsbehörden oder im Falle von Beschwerden gegenüber Betroffenen als Beleg zu dienen. Diese Dokumentation bildet außerdem die Grundlage für interne Audits und unterstützt die kontinuierliche Verbesserung des Datenschutzmanagementsystems.

Die DSGVO sieht zwei wesentliche Methoden vor, die als Faktor für die Erfüllung der in Art. 32 Abs. 1 DSGVO genannten TOM herangezogen werden können, nämlich genehmigte Verhaltensregeln und zertifizierte Verfahren. Dies bedeutet im Kontext von Cloud-Computing, dass die Wahl eines gemäß Art. 42 DSGVO zertifizierten Anbieters oder die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO durch den Anbieter ausreichen kann, um der Nachweispflicht zu genügen.[86]

Unter den Verhaltensregeln gemäß Art. 40 DSGVO versteht man freiwillige Regeln, die aufgestellt werden, um die praktische Umsetzung der DSGVO zu erleichtern. Hierunter fallen beispielweise Regelungen zur fairen und transparenten Verarbeitung personenbezogener Daten.[87] Da die Verarbeitung personenbezogener Daten in der Cloud ohnehin eine umfassende und strenge Regelung erfordert, sollten spezifische Verhaltensregeln bereits im Auftragsverarbeitervertrag festgehalten werden. Was genau in einem solchen Vertrag vereinbart werden sollte, wird in dieser Arbeit unter „7.2.3 Vertragsgestaltung“ speziell behandelt.

Unter anderem muss der Cloud-Anbieter einige Voraussetzungen erfüllen, um als DSGVO-konformer Auftragsverarbeiter überhaupt in Frage zu kommen. Was gemäß Art. 42 DSGVO unter einem zertifizierten Anbieter zu verstehen ist und was bei der Auswahl eines Anbieters noch beachtet werden muss, wird folgend behandelt.

[86] Vgl. Art. 32 Abs. 3 DSGVO.
[87] Vgl. Art 40 Abs. 2 lit. a DSGVO.

7.2.2 Auswahl Cloud-Anbieter

Die einheitliche DSGVO der Europäischen Union spielt eine entscheidende Rolle bei der Auswahl von Cloud-Computing-Anbietern und deren Standorten. Vor dem Hintergrund einer immer weiter voranschreitenden digitalen Transformation in Unternehmen und Behörden wurde die bereits seit 1995 existierende Datenschutz-Richtlinie (95/46/EG) von der DSGVO, welche am 25. Mai 2018 in Kraft getreten ist, abgelöst. Die Verordnung ist im Gegensatz zur Richtlinie unmittelbar geltendes Recht und konnte so eine Vereinheitlichung des Datenschutzes in allen EU-Mitgliedstaaten bewirken. Es ist deshalb sehr von Vorteil, einen Anbieter im EU-Raum auszusuchen, da hier die DSGVO ohnehin gilt. Anders stellt sich die Situation bei der Übermittlung personenbezogener Daten an Auftragsverarbeiter mit Datenverarbeitungsstandorten außerhalb der EU dar. Hier muss besonders darauf geachtet werden, dass die Anforderungen zumindest der DSGVO entsprechen und auch im Vertrag festgehalten werden.[88]

Damit ein vertrauenswürdiger Cloud-Anbieter ausgewählt werden kann, sind Datenschutz-Audits und Zertifizierungen unerlässlich. Datenschutz-Audits sind notwendig, um regelmäßig die Einhaltung der Datenschutzstandards zu überprüfen und potenzielle Schwachstellen aufzudecken. Anforderungen an Cloud-Computing werden national und international durch verschiedene Normen und Standards definiert, z. B.:

- ISO/IEC 27001, 27017 und 27018
- BSI Anforderungskatalog Cloud-Computing (C5)
- Cloud Security Alliance: Cloud Controls Matrix.

Zertifizierungen, wie beispielsweise die ISO 27001, werden von der Internationalen Organisation für Normung entwickelt und bieten eine standardisierte Methode zur Bewertung und Bestätigung der Wirksamkeit von Datenschutzmaßnahmen in der Cloud. Durch die Vergabe eines solchen Zertifikats ist eine Prüfung durch einen BSI zertifizierten Auditor erforderlich. Dieser führt eine Dokumentenprüfung, eine

[88] Vgl. Hennrich, Cloud-Computing nach der Datenschutz-Grundverordnung, S. 144 – 145.

Vor-Ort-Inspektion und die Erstellung eines Auditberichts durch, welcher durch die Zertifizierungsstelle beim BSI geprüft wird. Während der Gültigkeitsdauer des Zertifikats finden jährlich Überwachungsaudits statt.[89]

Der BSI-Anforderungskatalog Cloud-Computing (C5) umfasst 17 Bereiche und basiert auf ISO/IEC 27001 sowie der Cloud Controls Matrix der Cloud Security Alliance. Die Einhaltung der C5-Anforderungen wird durch einen SOC 2-Bericht nachgewiesen, der auf dem international anerkannten ISAE 3000-Testat basiert. Die Produktsicherheitsanforderungen leiten sich aus dem EU Cybersecurity Act ab.[90]

Die Cloud Security Alliance bietet mit der Cloud Controls Matrix einen Kontrollrahmen für Cloud-Computing, der Sicherheitsprinzipien und Best Practices in 16 Themenbereichen strukturiert.[91]

Bei Unternehmen aus den Vereinigten Staaten als Auftragsverarbeiter sollte die Liste der zertifizierten Unternehmen des EU-U. S. Data Privacy Framework (EU-U. S. DPF) beachtet werden. Die Europäische Kommission hat am 10. Juli 2023 den Angemessenheitsbeschluss für das EU-U. S. DPF, als Nachfolger des „Privacy Shields", angenommen, welcher für Erleichterung der Übermittlung von personenbezogenen Daten von EU-Unternehmen in die Vereinigten Staaten sorgt. Dabei wird sichergestellt, dass EU-Bürger weiterhin wirksame Garantien und Schutzmaßnahmen gemäß europäischem Recht, also der DSGVO, erhalten, wenn ihre Daten in die Vereinigten Staaten übertragen werden. Zertifizierte Unternehmen müssen

- den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission, des Department of Transportation oder einer anderen anerkannten US-Behörde unterliegen,
- öffentlich erklären, dass sie die Grundsätze einhalten und

[89] Vgl. BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Zertifizierungsschema, S. 8, Anlage 11.
[90] Vgl. BSI, Cloud Computing Compliance Criteria Catalogue – C5:2020, S. 16- 17, Anlage 12.
[91] Vgl. Schläger, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 635, Rn. 185.

- ihre Datenschutzrichtlinien gemäß den Grundsätzen öffentlich bekannt machen und vollständig umsetzen.

Unternehmen, die die Grundsätze nicht mehr einhalten, werden von der Liste gestrichen. Diese Streichungen werden öffentlich zugänglich gemacht.[92]

Bei der Auswahl eines Cloud-Dienstleisters ist zudem auch die physische Sicherheit der Rechenzentren zu beachten. Ein gut gesicherter Standort verhindert unbefugten Zutritt, minimiert das Risiko von physischen Schäden und stellt sicher, dass Daten auch in Krisensituationen geschützt bleiben. Dies umfasst Maßnahmen wie beispielsweise Zugangskontrollen, Brandschutz oder eine Notstromversorgung.[93]

7.2.3 Vertragsgestaltung

Trotz Auswahl eines geeigneten Cloud-Anbieters sind dennoch bestimmte Themenbereiche vertraglich zu regeln. Cloud-Anbieter müssen durch den Auftraggeber vertraglich zur Einhaltung von Mindeststandards verpflichtet werden. In der Vertragsgestaltung sollten Service Level Agreements festgelegt werden, die die Verantwortlichkeiten und Verpflichtungen des Cloud-Anbieters im Hinblick auf die Sicherheit und den Datenschutz der in der Cloud gespeicherten Daten definieren. Es muss ein Vertrag ausgearbeitet werden, der gemäß Art. 28 Abs. 3 DSGVO zudem folgende Aspekte abdeckt:

- Gegenstand und Dauer der Verarbeitung

Der Vertrag muss den genauen Gegenstand der Datenverarbeitung klar definieren, einschließlich einer Beschreibung der Tätigkeiten wie z. B. Gehaltsdatenverarbeitung oder IT-Hosting. Abweichungen bedürfen der schriftlichen Zustimmung des Auftraggebers. Die Dauer der Verarbeitung ist ebenfalls festzulegen.

[92] Vgl. International Trade Administration/U.S. Department of Commerce, Data Privacy Framework (DPF) Program, Overview, (o. S.), Anlage 13.
[93] Vgl. Hennrich, Cloud-Computing nach der Datenschutz-Grundverordnung, S. 190 – 191.

- Art und Zweck der Verarbeitung

Zudem muss der Vertrag die konkreten Verarbeitungsarten wie das Erfassen, Speichern, Organisieren, Anpassen oder Verändern, Auslesen, Abfragen, Verbreiten, Abgleichen oder Verbinden, Einschränken, Löschen oder Vernichten von personenbezogenen Daten sowie den spezifischen Zweck der Verarbeitung genau beschreiben, um eine Zweckentfremdung zu vermeiden.

- Art der personenbezogenen Daten

Des Weiteren muss der Vertrag klar festlegen, welche Arten von personenbezogenen Daten verarbeitet werden. Diese Daten können nach ihrem Inhalt oder ihrer Funktion kategorisiert werden, zum Beispiel in Identifikationsdaten wie Name, Adresse, Geburtsdatum und Ausweisnummern, in Kontaktdaten wie Telefonnummern und E-Mail-Adressen oder in Gesundheitsdaten wie medizinische Befunde, Diagnosen und Behandlungspläne. Es sollte auch sichergestellt werden, dass der Auftragnehmer nur die Datenarten verarbeiten darf, die für den festgelegten Zweck erforderlich sind. Für die Verarbeitung zusätzlicher Daten ist eine gesonderte vertragliche Vereinbarung sowie die Zustimmung des Auftraggebers notwendig.

- Kategorien von betroffenen Personen

Weiterhin ist es wichtig, dass der Vertrag klar definiert, welche Personengruppen von der Datenverarbeitung betroffen sind. Dies könnten beispielsweise Mitarbeiter, Bürger oder Dritte sein.

- Pflichten und Rechte des Verantwortlichen

Es muss klar definiert werden, dass der Auftraggeber als der datenschutzrechtlich Verantwortliche im Sinne der DSGVO agiert. Dieser bestimmt den Zweck und die Mittel der Datenverarbeitung und trägt die rechtliche Verantwortung für die Einhaltung der Datenschutzvorschriften. Der Verantwortliche bleibt außerdem dafür zuständig, die Rechte der betroffenen Personen (z.B. Auskunftsrechte, Recht auf Berichtigung und Löschung), zu wahren. Zudem muss das Recht auf Weisung

durch den Auftraggeber geregelt werden, so dass der Auftraggeber dem Auftragnehmer Weisungen erteilen kann, die sich auf alle Aspekte der Datenverarbeitung beziehen können.

- Verpflichtung der Beschäftigten zur Vertraulichkeit (ähnlich dem heutigen Datengeheimnis § 53 BDSG)

Der Auftragnehmer muss sich vertraglich dazu verpflichten, dass seine Beschäftigten zur Vertraulichkeit geschult und verpflichtet sind. Diese Verpflichtung sollte so gefasst sein, dass sie über das Vertragsende sowie das Ende des Beschäftigungsverhältnisses zwischen Auftragnehmer und seinen Beschäftigten hinaus gilt.

- Umsetzung und Dokumentation angemessener technischer und organisatorischer Schutzmaßnahmen

Gemäß Art. 32 DSGVO ist der Auftragnehmer verpflichtet, angemessene TOM umzusetzen, um ein hohes Schutzniveau der verarbeiteten personenbezogenen Daten zu gewährleisten. Der Vertrag muss festlegen, dass diese Maßnahmen dokumentiert werden und der Auftraggeber auf Verlangen Einsicht in diese Dokumentation erhält. Zudem müssen diese Schutzmaßnahmen regelmäßig überprüft und an den Stand der Technik sowie an die spezifischen Risiken angepasst werden. Die TOM sollten dem Vertrag als Anhang beigefügt werden.

- Regelung des Einsatzes von Unterauftragnehmern

Der Vertrag muss regeln, dass der Auftragnehmer Unterauftragnehmer nur mit vorheriger ausdrücklicher schriftlicher Zustimmung gemäß Art. 28 Abs. 2 DSGVO des Auftraggebers einsetzen darf. Dies schützt den Auftraggeber davor, dass personenbezogene Daten unkontrolliert an Dritte weitergegeben werden. Es ist zudem zu regeln, dass der Auftragnehmer sicherzustellen hat, dass Unterauftragnehmer dieselben datenschutzrechtlichen Verpflichtungen erfüllen wie der Hauptauftragnehmer selbst. Jede Änderung im Hinblick auf den Einsatz von Unterauftragnehmern ist dem Auftraggeber mitzuteilen und gegebenenfalls muss eine neue Zustimmung eingeholt werden.

- Unterstützung des Verantwortlichen bei der Wahrnehmung der Rechte der betroffenen Personen,

Der Vertrag sollte festlegen, dass der Auftragnehmer den Verantwortlichen aktiv bei der Erfüllung der Betroffenenrechte aus Art. 15 bis 22 DSGVO unterstützt. Dies umfasst unter anderem das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie das Widerspruchsrecht. Es ist wichtig, eine klare Frist zu definieren, innerhalb derer der Auftragnehmer auf Anfragen des Auftraggebers reagiert, da Informationen auf Anfragen zu Betroffenenrechten unverzüglich, spätestens aber innerhalb eines Monats, zur Verfügung zu stellen sind.[94]

- Unterstützung des Verantwortlichen bei der Meldung von Datenpannen und der Durchführung von Datenschutz-Folgenabschätzungen

Für den Fall von Datenpannen ist zu regeln, dass der Auftragnehmer den Auftraggeber unverzüglich über jede festgestellte Datenschutzverletzung informiert, die die im Auftrag verarbeiteten personenbezogenen Daten betrifft. Der Vertrag sollte dabei festlegen, wie diese Meldung zu erfolgen hat und welche Informationen dabei zu übermitteln sind. Es ist schriftlich festzuhalten, dass der Auftragnehmer den Verantwortlichen bei der Einhaltung der gesetzlichen Meldepflichten gegenüber der Aufsichtsbehörde und den betroffenen Personen gemäß Art. 33 und 34 DSGVO zu unterstützen hat. Des Weiteren hat er den Auftragnehmer bei der Durchführung einer DSFA zu unterstützen, insbesondere durch die Bereitstellung relevanter Informationen über die Datenverarbeitung und die eingesetzten Schutzmaßnahmen.

- Rückgabe oder Löschung personenbezogener Daten nach Beendigung des Auftrags

Nach Beendigung des Vertragsverhältnisses muss der Auftragnehmer verpflichtet sein, alle personenbezogenen Daten, die im Rahmen des Auftrags verarbeitet wurden, entweder zu löschen oder zurückzugeben. Es ist sicherzustellen, dass auch

[94] Vgl. Art. 12 Abs. 3 DSGVO.

Unterauftragnehmer alle relevanten Daten nach Vertragsende löschen oder zurückgeben. Eine Dokumentations- und Nachweispflicht für die Löschung der Daten sollte ebenfalls vertraglich festgelegt werden.

- Kontrollrechte des Verantwortlichen und entsprechende Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters

Dem Auftraggeber muss zudem das Recht eingeräumt werden, regelmäßige Audits oder Inspektionen beim Auftragnehmer durchzuführen, um die Einhaltung der datenschutzrechtlichen Vorgaben zu überprüfen. Der Auftragnehmer muss verpflichtet werden, bei solchen Audits umfassend mitzuwirken und Zugang zu relevanten Informationen, Dokumentationen und Systemen zu gewähren.

- Hinweispflicht bei Weisungen, die gegen datenschutzrechtliche Vorschriften verstoßen

Abschließend muss der Auftragnehmer vertraglich gebunden sein, den Auftraggeber unverzüglich zu informieren, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt.

Insgesamt trägt die Vertragsgestaltung einen wesentlichen Teil zur Gewährleistung der Datenschutzgrundsätze bei. Durch Festlegen der spezifischen Zwecke und Arten der Daten, die verarbeitet werden sollen, werden Grundsätze wie Zweckbindung und Datenminimierung sichergestellt. Durch genaue Regelungen zum Einsatz von Unterauftragnehmern kann sichergestellt werden, dass Daten nicht unbewusst außerhalb der EU verarbeitet werden. Zudem trägt der Vertrag nicht nur der Rechenschaftspflicht bei, sondern verpflichtet den Auftragsverarbeiter zur Einhaltung dieser speziellen Vereinbarungen. Als Muster für einen Auftragsverarbeitervertrag kann das vom Landesbeauftragen für Datenschutz und Informationssicherheit (LfDI) verwendet werden.[95]

[95] Vgl. LfDI, Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO, Anlage 14.

7.2.4 Checkliste für organisatorische Maßnahmen

Abschließend zu den organisatorischen Maßnahmen folgt auch hier eine Checkliste, die in der Praxis als Hilfestellung bei der Entscheidung über eine Auslagerung der Daten in die Cloud eingesetzt werden kann.

Allgemeine organisatorische Maßnahmen

☐ Der Anbieter verfügt über einen Datenschutzbeauftragten, welcher als zentraler Ansprechpartner bei datenschutzrechtlichen Fragen dient.

☐ Der Anbieter führt regelmäßige Schulungen zur Sensibilisierung der eigenen Mitarbeiter durch und bietet Schulungen im Umgang mit der zur Verfügung gestellten Leistung auch der Behörde als Nutzerin an.

Sicherheitsrichtlinien- und verfahren

☐ Der Anbieter verfügt über klar definierte Sicherheitsrichtlinien, die den Schutz von Daten und die Einhaltung von Datenschutzbestimmungen sicherstellen.

Audit und Compliance

☐ Es handelt sich um einen gemäß Art. 42 DSGVO zertifizierten Anbieter.

☐ Regelmäßige interne und externe Audits zur Überprüfung der Einhaltung von Sicherheits- und Datenschutzrichtlinien werden durchgeführt.

☐ Transparente Berichterstattung und Dokumentation der Audit-Ergebnisse sind verfügbar. (Bspw. aus Zertifizierungsverfahren)

Notfallmanagement und Kommunikation

☐ Es gibt festgelegte Prozesse für die Meldung, Untersuchung und Behebung von Sicherheitsvorfällen.

☐ Klare Kommunikationswege und Meldepflichten sind etabliert, um sicherzustellen, dass alle relevanten Parteien im Falle eines Sicherheitsvorfalls umgehend informiert werden.

☐ Die aktuelle Software entspricht den Sicherheitsstandards.

☐ Systeme zur Erkennung und Verhinderung von Angriffen auf die Cloud-Infrastruktur sind implementiert.

☐ Es wird sichergestellt, dass die Daten vollständig und sicher gelöscht werden können, wenn die Dienstleistung beendet wird.

Physische Sicherheit

☐ Physische Zugänge zu den Rechenzentren werden streng kontrolliert.

☐ Es gibt ausreichende Brandschutzmaßnahmen (bspw. Kühlung der Datenträger inklusive Klimakontrollen, Brandfrühwarnsysteme).

☐ Es ist eine redundante Stromversorgung vorhanden.

Vertragsgestaltung

☐ Der Vertrag entspricht den Anforderungen der DSGVO. Es wurden alle Aspekte des Art. 28 Abs. 3 DSGVO vertraglich geregelt sowie (falls notwendig) weitere Regelungen aufgenommen, wie bspw. bei ausländischen Auftragsverarbeiter.

☐ Organisatorische und technische Maßnahmen des Anbieters werden explizit im Anhang des Vertrages aufgeführt.

8. Zukunftsperspektive

Bei der Untersuchung der verschiedenen Optionen für Cloud-basierte Lösungen in öffentlichen Institutionen wird deutlich, dass Cloud-Computing zahlreiche Vorteile bietet, jedoch auch große Herausforderungen mit sich bringt. Während datenschutzbezogene Herausforderungen durch die in der Arbeit behandelten TOM weitgehend gelöst werden können, bleibt die Gefahr der Abhängigkeit von externen Anbietern bestehen. Eine mögliche zukunftsorientierte Lösung wäre die Entwicklung und Nutzung eigener Cloud-Systeme durch den öffentlichen Sektor. Bereits 2021 erkannte der IT-Planungsrat, welcher das zentrale politische Steuerungsgremium für die Digitalisierung der öffentlichen Verwaltung in Deutschland ist, dass die Entwicklung eigener Cloud-Systeme eine vielversprechende Alternative zur Auslagerung in externe Cloud-Dienste sein könnte. Der IT-Planungsrat entwickelte daher die Deutsche Verwaltungscloud-Strategie als eine föderale Initiative, die eine einheitliche, sichere und leistungsfähige Cloud-Infrastruktur für die öffentliche Verwaltung in Deutschland schaffen soll. Ziel ist es, eine Plattform bereitzustellen, die es Behörden ermöglicht, IT-Ressourcen, Anwendungen und Daten effizient und

sicher zu verwalten. Dabei liegt ein besonderes Augenmerk auf der Einhaltung hoher Datenschutz- und Sicherheitsstandards, die speziell auf die Bedürfnisse des öffentlichen Sektors zugeschnitten sind. Die Deutsche Verwaltungscloud ist mehr als nur eine technische Lösung; sie verkörpert eine zukunftsorientierte Strategie, die darauf abzielt, die digitale Souveränität der öffentlichen Hand zu stärken und gleichzeitig den Weg für innovative Verwaltungsdienste zu ebnen.[96]

Solche staatlich kontrollierten Cloud-Infrastrukturen würden es ermöglichen, die Kontrolle vollständig in den Händen der öffentlichen Verwaltung zu behalten, insbesondere in Bezug auf Datensicherheit und Datenschutz. Die Schaffung einer eigenen Cloud-Lösung könnte somit die kritische Abhängigkeit von externen Anbietern weiter verringern und eine höhere Souveränität gewährleisten, was eine langfristig stabile und sichere Grundlage für die digitale Verwaltung in Deutschland darstellen würde. Durch die vollständige Kontrolle der Daten wäre sichergestellt, dass Datenschutzrichtlinien tatsächlich eingehalten werden.[97] Darüber hinaus verfolgt die Deutsche Verwaltungscloud-Strategie das Ziel, föderale Standards und offene Schnittstellen zu nutzen, um eine nahtlose Interoperabilität zwischen unterschiedlichen IT-Systemen in der Verwaltung zu gewährleisten. Durch diese Strategie können Behörden Daten leichter und sicher austauschen, was eine nahtlose Zusammenarbeit ermöglichen würde.[98]

Derzeit befindet sich die Deutsche Verwaltungscloud in einer fortgeschrittenen Entwicklungsphase, wobei erste Pilotprojekte durchgeführt werden. Der IT-Planungsrat arbeitet intensiv daran, die notwendigen technischen und rechtlichen Rahmenbedingungen für den flächendeckenden Einsatz der Verwaltungscloud zu schaffen. Dabei steht die Entwicklung robuster Sicherheits- und Datenschutzkonzepte im Vordergrund, um den besonderen Anforderungen der öffentlichen Verwaltung gerecht zu werden.[99]

[96] Vgl. IT-Planungsrat, Deutsche Verwaltungscloud-Strategie, S. 3 u. S. 7, Anlage 15.
[97] Vgl. IT-Planungsrat, Deutsche Verwaltungscloud-Strategie, S. 4, Anlage 15.
[98] Vgl. IT-Planungsrat, Deutsche Verwaltungscloud-Strategie, S. 7 u. S. 10, Anlage 15.
[99] Vgl. IT-Planungsrat, Umsetzungsbericht und -konzept Projekt DVC, S. 3 u. S. 9, Anlage 16.

9. Fazit

Zielsetzung dieser Arbeit war es, wirksame Maßnahmen zu ermitteln und darzustellen, die den Schutz sensibler Daten und die Einhaltung geltender Datenschutzbestimmungen in dieser zunehmend digitalisierten Umgebung gewährleisten. Um diese Zielsetzung zu erreichen, wurde zuerst verdeutlicht, welche spezifischen Risiken und Herausforderungen im Zusammenhang mit Datenschutz in der Cloud im öffentlichen Sektor bestehen, wodurch die erste Forschungsfrage beantwortet werden konnte. Es wurde zum einen das Risiko der gemeinsamen Nutzung gepoolter IT-Ressourcen behandelt, was Herausforderungen hinsichtlich der Datentrennung und des Zugriffs mit sich bringt. Des Weiteren wurden Sicherheitsmängel auf verschiedenen Ebenen, wie beispielsweise auf der Rechenzentrumsebene, erwähnt, wobei durch ein unzureichendes Sicherheitskonzept die physische Sicherheit der Daten gefährdet werden könnte. Zudem wurde thematisiert, dass die grenzüberschreitende Datenverarbeitung eine besondere Herausforderung darstellt, da die DSGVO außerhalb der EU möglicherweise nicht greift. Weiterhin wurde aufgegriffen, dass die Abhängigkeit von Cloud-Anbietern ein erhebliches Risiko aufzeigt, was zu Kontrollverlust führen kann. Abschließend wurde die Bedrohung durch Cyberattacken, wie etwa durch Malware, thematisiert, da dadurch die Sicherheit der in der Cloud gespeicherten sensiblen Daten gefährdet werden kann.

Des Weiteren wurde untersucht, welche technischen und organisatorischen Maßnahmen besonders gut geeignet sind, um einen effektiven Datenschutz in der Cloud zu gewährleisten und die Integrität sensibler Daten zu bewahren. Dadurch konnte die zweite Forschungsfrage beantwortet werden. Im Fokus standen insbesondere die Implementierung moderner Technologien wie die Verschlüsselung, die den Schutz der Daten vor unbefugtem Zugriff gewährleistet, sowie organisatorische Vorkehrungen, die sicherstellen, dass Datenschutzpraktiken systematisch und nachhaltig in die alltäglichen Abläufe integriert werden.

Das Ergebnis dieser Untersuchung zeigt, dass durch die gezielte Kombination von technischen und organisatorischen Maßnahmen eine hohe Datenschutzkonformität erreicht werden kann. Im Rahmen der technischen Maßnahmen wurde neben der

Pseudonymisierung und Anonymisierung von Daten erarbeitet, wie Verschlüsselungstechnologien in der Praxis konkret gestaltet und implementiert werden sollten, um einen optimalen Schutz der Daten sicherzustellen. Dazu gehören die Verwendung von starken Verschlüsselungsalgorithmen, die eine Entschlüsselung ohne den passenden Schlüssel praktisch unmöglich machen, sowie die konsequente Verschlüsselung sowohl im Ruhezustand als auch während der Übertragung. Ergänzend dazu wurde das Zugangs- und Zugriffsmanagement behandelt, das sicherstellt, dass nur autorisierte Personen auf sensible Daten zugreifen können, wobei moderne Authentifizierungsverfahren und die Prinzipien der minimalen Rechtevergabe zum Einsatz kommen. Abschließend zu den technischen Maßnahmen wurde die endgültige Löschung von Daten auf Cloud-Servern thematisiert, die sichergestellt werden muss, um Betroffenenrechte als auch die Grundsätze des Datenschutzes zu gewährleisten.

Auf organisatorischer Ebene hat sich gezeigt, dass die Bestellung eines Datenschutzbeauftragten, der regelmäßig die Einhaltung der Datenschutzvorgaben überprüft und die Durchführung von Datenschutz-Folgenabschätzungen entscheidend dazu beitragen, Risiken proaktiv zu steuern. Ebenso wurde erarbeitet, wie die sorgfältige Auswahl geeigneter Cloud-Anbieter erfolgen sollte, wobei Kriterien wie der Standort oder Zertifizierungen des Anbieters im Mittelpunkt standen. Eine DSGVO-konforme Vertragsgestaltung wurde als wesentlich erachtet, um sicherzustellen, dass alle datenschutzrechtlichen Anforderungen klar definiert und rechtlich bindend sind.

Insgesamt konnte festgestellt werden, dass durch die Integration dieser technischen und organisatorischen Maßnahmen die Nutzung von Cloud-Services in öffentlichen Institutionen nicht nur sicher, sondern auch effizient gestaltet werden kann. Um damit die letzte Forschungsfrage zu beantworten, nämlich wie die Cloud-Technologie im öffentlichen Sektor trotz dieser Herausforderungen effektiv genutzt werden kann, um die Digitalisierung voranzutreiben und ohne die datenschutzrechtlichen Anforderungen zu gefährden, muss eine strenge Prüfung der in dieser Arbeit behandelten TOM unterzogen und konsequent umgesetzt werden. Eine kritische Prüfung der TOM ist notwendig, um einen angemessenen Datenschutz zu gewähr-

leisten. Es ist genau abzuwägen, ob und wie Cloud-Services eingesetzt werden sollen und wo möglicherweise eigene Lösungen entwickelt werden können, um die volle Kontrolle über den Datenschutz zu bewahren. Eine sorgfältige Planung und Umsetzung der Maßnahmen schützt nicht nur die Datenschutzrechte der betroffenen Personen, sondern schafft auch eine Grundlage für den sicheren Einsatz von Cloud-Diensten im öffentlichen Sektor, was die Modernisierung und Effizienzsteigerung durch Digitalisierung vorantreiben kann.

Unter Betrachtung der Datenschutzaspekte ist die interne Cloud im öffentlichen Sektor das bevorzugte Modell für die Verarbeitung personenbezogener Daten. Sie bietet Kontrolle, da sie ausschließlich von einer Organisation genutzt wird und erhöhte Datensicherheit durch die Nutzung interner Speicherressourcen. Dennoch sind interne Lösungen für alle Bereiche der Verwaltung sehr zeitaufwändig und kostenintensiv, da Hardware und verschiedene Software für unterschiedliche Ämter benötigt werden und gepflegt werden müssen. Oft fehlt hierfür das benötigte Personal, besonders in kleineren Kommunen.[100] Daher bietet sich eine private Cloud-Lösung bei einem DSGVO-konformen Anbieter an.

Trotzdem bleibt die Tatsache bestehen, dass der Cloud-Anbieter die physische Kontrolle über die Daten hat. Dies stellt stets ein Risiko dar, da trotz aller vertraglich geregelten Vorsichtsmaßnahmen und Vereinbarungen Probleme auftreten können. Durch die physische Gewalt des Anbieters bleibt auch stets der Kontrollverlust ein Risiko, dem sich öffentliche Institutionen aussetzen. Insbesondere bei der Löschung von Daten kann eine Behörde nicht mit Sicherheit überprüfen, ob die Daten tatsächlich unwiderruflich gelöscht wurden. Es ist nicht nachvollziehbar, ob Daten möglicherweise noch auf anderen Servern gespeichert wurden oder rekonstruiert werden könnten. Diese Unsicherheiten und das Risiko einer nicht ausreichenden Transparenz gegenüber Nutzern externer Cloud-Dienste sind besonders problematisch. Selbst bei strikten Verträgen und detaillierten Vereinbarungen bleibt die Kontrolle über die Daten letztlich beim Cloud-Anbieter. Cloud-Lösungen

[100] Vgl. Landtag von Baden-Württemberg, Drucksache 17 / 6100, S. 57.

externer Anbieter sind daher trotz der vielen Vorteile mit großer Vorsicht zu betrachten. Der Datenschutz sollte nicht durch die Bequemlichkeit externer Dienstleister gefährdet werden. Eine datenschutzkonforme Lösung bei einem Drittanbieter stellt dabei die Verwendung einer Sealed-Cloud-Lösung dar, die bereits verschiedene Verschlüsselungstechnologien umsetzt und so den Zugriff auf Daten selbst für Dienstanbieter verhindert. Dadurch können Risiken bei der Anbieterabhängigkeit weitgehend gemindert werden.

Abschließend lässt sich sagen, dass Cloud-Computing großes Zukunftspotenzial im öffentlichen Sektor hat. Durch die Entwicklung und den Einsatz einer Deutschen Verwaltungscloud könnten nicht nur bestehende Risiken verringert, sondern auch erhebliche Effizienzgewinne erzielt werden, die zudem die Digitalisierung der öffentlichen Verwaltung voranbringen. Mit einer sorgfältigen Planung und Umsetzung kann die Deutsche Verwaltungscloud eine zentrale Säule für die zukunftssichere digitale Verwaltung in Deutschland werden.

Literaturverzeichnis

Auer-Reinsdorff, Astrid/Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019

BfDI, Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, Version 1.1-BfDI, 2019, (o. S.) https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=5 (Abruf am 25.08.2024).

Borges, Georg/Werner, Brigitte, Identitätsmanagement im Cloud Computing, 1. Auflage, 2018.

BSI, Technische Richtlinie TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Stand 02. Februar 2024, 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10 (Abruf am 21.08.2024).

BSI, Cloud Computing Compliance Criteria Catalogue – C5:2020, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/C5_2020.pdf?__blob=publicationFile&v=3 (Abruf am 23.08.2024).

BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Zertifizierungsschema Version 2.1, 2019, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile (Abruf am 23.08.2024).

Committee on National Security Systems, Glossary, CNSSI No. 4009, 2015, https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf (Abruf 22.08.2024).

DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Stand 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (Abruf am 25.08.2024).

Ebers, Martin, Legal Tech, Stichwort Kommentar, 1. Auflage, Edition 2, 2023.

ENISA, Data Pseudonymisation: Advanced Techniques and Use Cases, Januar 2021, (E-Book).

Gola, Peter/Heckmann, Dirk, DS-GVO, Kommentar, 3. Auflage, 2022.

Grance, Timothy/Mell, Peter, NIST Special Publication 800-145, The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (Abruf am 21.08.2024).

Heckmann, Dirk, Internetrecht und Digitale Gesellschaft, Band 4, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, 2016, (E-Book).

Hennrich, Thorsten, Cloud-Computing nach der Datenschutz-Grundverordnung, 1. Auflage, 2023.

Hesseler, Martin/Görtz, Marcus, Basiswissen ERP-Systeme, Auswahl, Einführung & Einsatz betriebswirtschaftlicher Standardsoftware, 2007, (E-Book).

Hornung, Gerrit /Schallbruch, Martin, IT-Sicherheitsrecht, 1. Auflage, 2021.

Huawei Technologies Co., Ltd., Cloud Computing Technology, 1. Auflage, 2023, (E-Book).

International Trade Administration, U.S. Department of Commerce, Data Privacy Framework (DPF) Program, Overview, (o. J.), https://www.dataprivacyframework.gov/framework-article/OVERVIEW (Abruf 24.08.2024).

IT-Planungsrat, Umsetzungsbericht und -konzept Projekt DVC, Beschluss 2023-36_DVC_Bericht, Stand 11.10.2023 https://www.it-planungsrat.de/fileadmin/beschluesse/2023/Beschluss2023-36_DVC_Bericht.pdf (Abruf am 27.08.2024).

IT-Planungsrat, Deutsche Verwaltungscloud-Strategie, Version 1.4.1, 17.11.2020 https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/Deutsche_Verwaltungscloud_Strategie.pdf;jsessionid=93E3BD660BA7DC81EDC9EDFBDEEEA6E1.live861?__blob=publicationFile&v=2 (Abruf am 27.08.2024).

Jansen, Wayne/Grance, Timothy, NIST, Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (Abruf am 21.08.2024).

LfDI, Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/200429_AVV-Muster_DE.pdf (Abruf am 25.08.2024).

NIST, Federal Information Processing Standards, 197: Advanced Encryption Standard (AES), 2001, updated 2023, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf (Abruf am 21.08.2024).

NIST, Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf (Abruf am 22.08.2024).

Paal, Boris/Pauly, Daniel A., DS-GVO, Beck'sche Kompakt-Kommentar, 3. Auflage, 2021.

Schläger, Uwe/Thode, Jan-Christoph, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, 2022, (E-Book).

Schneider, Jochen, Handbuch EDV-Recht, 5. Auflage, 2017**.**

Seckelmann, Margrit, Digitalisierte Verwaltung Vernetztes E-Government, 2. Auflage, 2019, (E-Book).

Spiecker, Indra/Bretthauer Sebastian, Dokumentation zum Datenschutz, Loseblatt, Stand: 94. Auflage, 2024.

Uniscon GmbH, Sealed Cloud - Hochsichere Cloud-Lösungen sogar für Geheimnisträger gem. § 203 StGB, (o. J.) https://www.bvdnet.de/wp-content/uploads/2016/11/Uniscon_Sealed_Cloud_BvD_Uniscon_170503.pdf (Abruf am 03.09.2024).

Wissenschaftliche Dienste des Deutschen Bundestages, Datenübermittlung an US-Ermittlungsbehörden auf Grundlage des CLOUD Acts im Geltungsbereich des EU-Datenschutzrechts, WD 3 - 3000 - 205/19 vom 20. August 2019, https://www.bundestag.de/resource/blob/662608/67dbc571f4d96be9adddcac99f016eb6/WD-3-205-19-pdf-data.pdf (Abruf am 21.08.2024).

Wollinger, Gina Rosa /Schulze, Anna, Handbuch Cybersecurity für die öffentliche Verwaltung, 1. Auflage, 2020.

Erklärung

Ich versichere, dass ich diese Bachelorarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet. Mir ist bekannt, dass meine Abschlussarbeit von Seiten der Hochschule mit einer Plagiatssoftware überprüft werden kann.

Ludwigsburg den 16. September 2024

Alina Sarah Kopf