TU WIEN Informatics

Territoriale Aspekte des Cloud Computing

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering/Internet Computing

eingereicht von

Gerd Saurer
Matrikelnummer 0025645

an der Fakultät für Informatik
der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 08. Jänner 2021

Unterschrift Verfasser/in	Unterschrift Betreuer/in

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Erklärung zur Verfassung der Arbeit

Gerd Saurer

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 08. Jänner 2021

Gerd Saurer

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kurzfassung

Heutzutage spielt Cloud Computing in der Informationstechnologie eine sehr wichtige Rolle. Viele Unternehmen möchten Ressourcen flexibler und effizienter einsetzen und dabei ihre Kosten senken. Um dies zu erreichen, ermöglicht Cloud Computing, den Betrieb von Anwendungen oder Infrastruktur (z.B. Rechenleistung, Speicherkapazität, usw.) an außenstehende Anbieter auszulagern.

Im Zusammenhang mit diesen Dienstleistungen bringt Cloud Computing zahlreiche Problemstellungen im Bereich des Vertrags- und Datenschutzrechtes mit sich, die in dieser Arbeit näher diskutiert werden.

Speziell das Löschen von Daten stellt eine Herausforderung dar, weil dieses nicht umfassend rechtlich geregelt und auch die technische Umsetzung problematisch ist. Der Schwerpunkt dieser Arbeit liegt daher in einer Betrachtung des Rechts auf das Löschen von Daten in der Cloud. Es werden existierende rechtliche Grundlagen sowie ein neuer Ansatz das „Recht auf Vergessenwerden“ erläutert. In diesem Zusammenhang werden die Erkenntnisse aus rechtlicher und technischer Sicht zusammengefasst und ein Ausblick gegeben, wie das Recht auf Vergessenwerden rechtlich und technisch umgesetzt werden könnte.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Abstract

Nowadays, cloud computing plays a very important role in information technology. Many companies would like to use resources more flexible and efficient while reducing their costs. To achieve this, cloud computing enables the operation of applications or infrastructure (e.g. computing power, storage capacity, etc.) to be outsourced to external providers.

In connection with these services, cloud computing brings numerous problems in the contract and data protection law with it, which are discussed in more detail in this work.

Particularly, the deletion of data is a challenge because it is not comprehensively regulated, and the technical implementation is problematic as well. The focus of this work lies on a consideration of the right to delete data in the cloud. Existing legal principles and a new approach, the "right to be forgotten", are explained. In this context, the findings are summarized from a legal and technical point of view and an outlook is given of how the right to be forgotten could be implemented legally and technically.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Inhaltsverzeichnis

KAPITEL 1 EINLEITUNG 1

KAPITEL 2 TECHNISCHE BETRACHTUNG DER CLOUD 3

2.1 Eigenschaften von Cloud Computing 3

2.2 Service-Modelle 6
2.2.1 Infrastructure as a Service (IaaS) 7
2.2.2 Platform as a Service (PaaS) 9
2.2.3 Software as a Service (SaaS) 10

2.3 Deployment-Modelle 11
2.3.1 Private Cloud 12
2.3.2 Community Cloud 13
2.3.3 Public Cloud 13
2.3.4 Hybrid Cloud 14

KAPITEL 3 RECHTLICHE BETRACHTUNG DER CLOUD 17

3.1 Zivil- und Vertragsrecht 17
3.1.1 Internationaler Charakter des Cloud-Vertrages, anwendbares Recht 17
3.1.2 Vertragstypologie und Vertragsmodelle 18
3.1.3 Gewährleistung und Haftung 19
3.1.3.1 Gewährleistung 19
3.1.3.2 Sorgfaltspflichten des Cloud-Providers 21
3.1.3.3 Haftung des Cloud Dienstleisters gegenüber seinen Kunden 21
3.1.3.4 Grenzen der Vertragsgestaltung und Haftungsbeschränkung 24
3.1.3.5 Wichtige Klauseln im Cloud-Vertrag 25

3.2 Datenschutzrecht 30
3.2.1 Internationaler Datenschutz 30
3.2.2 Datenschutzrechtliche Stellung des Cloud Anbieters 33
3.2.3 Rechtliche Anforderungen 35
3.2.3.1 Zulässige Datenverarbeitung durch den Auftraggeber 35
3.2.3.2 Sorgfältige Auswahl des Cloud-Providers 36
3.2.3.3 Erfüllung Datensicherheitsmaßnahmen 37
3.2.3.4 Stellung des Subdienstleisters 38

3.3 Standards und Frameworks 39

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

3.3.1 ISO Standards 40
3.3.1.1 ISO 27017 45
3.3.1.2 ISO 27018 45
3.3.2 AICPA – SOC 1-3 46
3.3.3 Cloud Security Alliance (CSA) 47
3.3.3.1 Security Guide 48
3.3.3.2 CSA Security, Trust and Assurance Registry (STAR) 49
3.3.4 Übersicht weltweit relevanter Standards und Zertifizierungen 51

KAPITEL 4 LÖSCHUNG VON DATEN IN DER CLOUD 58

4.1 Rechtliche Aspekte 58
4.1.1 Das Recht auf Vergessenwerden 58
4.1.1.1 Problemstellung und Definition 58
4.1.1.2 Datenschutzrichtlinie (95/46/EG) 59
4.1.1.3 Datenschutz-Grundverordnung (DSGVO) 60
4.1.1.4 Urteil des EuGHs zu C 131/12 65
4.1.1.5 Das Recht auf Löschung im österreichischen Datenschutzgesetz 68
4.1.1.6 Kritik des Rechtes auf Vergessenwerden 70
4.1.1.7 Max Schrems und Europe v. Facebook 70
4.1.1.8 Das Privacy Shield Abkommen 75

4.2 Technische Aspekte 77
4.2.1 Technische Herausforderungen 77
4.2.2 Existierende Technologien 82
4.2.2.1 X-pire! 83
4.2.2.2 X-pire 2.0 86
4.2.2.3 Vanish System 89
4.2.2.4 Ephemerizer 96
4.2.2.5 Data Revocation Service (DRS) 97
4.2.2.6 Secure Overlay Cloud Storage (FADE) 101
4.2.2.7 Digitales Wasserzeichen 104
4.2.2.8 Digital Rights Management (DRM) 107
4.2.2.9 User basiertes semantisches Rechtemodel zur Validierung von Inhalten 110

4.3 Fazit und Lösungsansätze 113
4.3.1 Mögliche rechtliche Ansätze 114
4.3.2 Mögliche technische Ansätze 114

KAPITEL 5 QUELLENVERZEICHNIS 116

5.1 Literatur 116

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

5.2 Rechtsgrundlagen & Relevante Judikatur 122

5.3 Zeitungsartikel und Presse 122

5.4 Internet 123

KAPITEL 6 ABBILDUNGSVERZEICHNIS 128

KAPITEL 7 TABELLENVERZEICHNIS 129

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 1
Einleitung

Cloud Computing hat in den letzten Jahren sehr stark an Bedeutung gewonnen. Das Konzept, einen Pool an Infrastruktur gemeinsam über ein globales Netzwerk nutzen zu können, ist hierbei jedoch nicht neu. Bereits in den sechziger Jahren wurde das Konzept eines „intergalactic computer networks“[1] durch J.C.R Licklinder beschrieben. Seine Vision war es, dass jeder über ein globales Netzwerk auf Programme und Daten zugreifen kann. Einer der Hauptgründe, warum sich dies zu diesem Zeitpunkt noch nicht verwirklichen ließ, war die fehlende Konnektivität, die erst in den späten 1990er Jahren ausreichend zur Verfügung stand.[2]

Seit dieser Zeit waren unterschiedliche technische Entwicklungen dafür verantwortlich, dass Applikationen modularer aufgebaut werden konnten. Diese Modularisierung erlaubte es Anwendungsentwicklern, gewisse Komponenten als Services auszulagern. Diese zentral zur Verfügung gestellten Services, konnten dann von unterschiedlichen Applikationen verwendet werden. In Verbindung mit der Weiterentwicklung des WWW und dem Ausbau der Infrastruktur (Netzwerk) entstand damit die Möglichkeit, so genannte Web Services zentral zur Verfügung zu stellen beziehungsweise eine Service-Oriented Architecture (SOA)[3] aufzubauen.[4]

---

[1] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolf. „Brief History of the Internet.“ Internet Society, (1997): 3

[2] ComputerWeekly. „A history of cloud computing.“ http://www.computerweekly.com/feature/A-history-of-cloud-computing (zugegriffen: 1.2.2020)

[3] Melzer, Ingo. Service-Orientierte Architekturen Mit Web Services. Heidelberg: Spektrum Akademischer Verlag GmbH, (2010): 10-13

[4] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.“ Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 1: Introduction to the Cloud

Eines der ersten Unternehmen, die sich diese neuen Methoden zu Nutze machten, war Amazon[5]. Bereits sehr früh erkannte Amazon, dass es viele Vorteile hatte, ihren Online Buch Shop auf einer SOA aufzubauen. Je nach Anforderung des Webshops, was es möglich, einzelne Services zu skalieren, aber auch einfach und schnell neue Services zur Verfügung stellen, welche danach in unterschiedlichen Bereichen integriert werden konnten. Speziell in der Zeit vor Weihnachten, wo sehr viele Bücher gekauft wurden, konnte die Kapazität für einzelne Services erhöht und nach Abdeckung der Spitze wieder heruntergefahren werden. Dieser Mechanismus erlaubte es, die gleiche Hardware für unterschiedliche Services zu benützen (z.B. Webshop und Buchhaltung), je nachdem, welche gerade benötigt wurden. Trotz dieser Möglichkeit musste die Hardware auf die Maximalanforderung des Unternehmens ausgelegt werden. Da die gesamte Infrastruktur trotzdem nur sehr selten benötigt wurde, überlegte man sich, wie die Ressourcen auch andere Unternehmen zur Verfügung gestellt werden konnten. Dies war die Gründungsidee von Amazon Web Services[6], welche 2002 eingeführt wurden. Hierbei handelte es sich um eine Anzahl an Cloud basierten Services (z.B. Speicher, Webservice), welche Anwender über ein Portal konfigurieren und zugreifen können. Dies war allgemein als die Geburtsstunde des heutigen Cloud Computing bezeichnet. Entwickler mussten sich nicht mehr selbst um den Betrieb der Hardware kümmern, sondern konnten einfach über ein Portal die gewünschten Services beziehen. Bereits 2006 wurde das Angebot durch Elastic Computer Cloud (EC2) erweitert, welche Kunden die Möglichkeit gab, ihre eigenen Server in der Cloud zu betreiben.[7]

Ein weiterer wichtiger Schritt war getan, als große Unternehmen wie Microsoft und Google 2009 begannen, ihre Softwareprodukte als Services in der Cloud zur Verfügung zu stellen. Diese Software as a Service (SaaS) Komponenten wie Business Productivity Online Suite (BPOS, heutiges Office 365) oder Google Apps machten es für Anwender sehr einfach, Applikationen über die Cloud zu beziehen, ohne sie selbst betreiben zu müssen.

---

[5] „Amazon.com“ https://www.amazon.com/ (zugegriffen: 27.10.2020)

[6] „Amazon Web Services (AWS).“ https://aws.amazon.com/ (zugegriffen: 1.5.2020)

[7] „Benjamin Black – EC2 Origins.“ http://blog.b3k.us/2009/01/25/ec2-origins.html (zugegriffen: 1.5.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Kapitel 2
Technische Betrachtung der Cloud

2.1 Eigenschaften von Cloud Computing

Heute wird zwischen unterschiedlichen Arten von Cloud Computing unterschieden, auf welche in dem nächsten Kapitel näher eingegangen wird. Wichtige Eigenschaften der unterschiedlichen Clouds, welche auch heute noch als Basis zur Kategorisierung verwendet werden, sind:

- On-Demand

  Anwender können Services innerhalb von kurzer Zeit eigenständig konfigurieren und verwenden. Die Provisionierung der Services erfolgt meist über eine API[8] oder ein Webportal. Sobald der Anwender eine Ressource angefragt hat, erfolgt eine automatisierte Bereitstellung der angefragten Komponenten. Der Zeitraum, bis die Services verwendet werden können ist unterschiedlich und hängt neben der Art der angefragten Services auch von dem jeweiligen Cloud-Provider und deren momentaner Auslastung ab. Üblicherweise handelt es sich dabei um wenige Sekunden oder Minuten. Das Service steht dem Anwender so lange zur Verfügung, bis dieser beschließt, es nicht mehr nutzen zu wollen. Eine Deprovisionierung der angefragten Services und Ressourcen wird ebenfalls über eine API oder ein Webportal angestoßen und erfolgt automatisch.[9]

[8] Fielding, Roy Thomas, Architectural Styles and the Design of Network-based Software Architectures, Dissertation University of California, (2000): 77

[9] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.“ Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 1: Introduction to the Cloud

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Geteilte Infrastruktur

  Cloud Computing verwendet meist das Konzept einer geteilten Infrastruktur. Dies bedeutet, dass mehrere Anwender auf einen großen Pool an Hardware gemeinsam zugreifen. Die einzelnen Benutzer werden dabei durch die Plattform logisch getrennt, damit Daten oder Services eines Kunden nicht von einem anderen zugegriffen werden können.[10]

  Betrachtet man dies am Beispiel von Speicher, so bietet der Cloud-Provider einen Pool an Datenspeicher an. Die verwendete Hardware ist für den Anwender transparent. Durch die Verwendung eines Pools können Daten von zwei unterschiedlichen Anwendern auf dem gleichen Speichermedium abgelegt werden. Der Cloud-Provider stellt in dem abstrahierten Service sicher, dass zu keinem Zeitpunkt Daten von anderen Anwendern sichtbar bzw. verwendbar sind.

  Im Bereich von Servern (z.B.: Web-Server) werden Virtualisierungstechnologien verwendet, um auf einem Server mehrere virtuelle Instanzen betreiben zu können und somit Skalierungsfaktoren zu nutzen.[11] In den letzten Jahren haben sich auch neue Konzepte der Virtualisierung, sogenannte Container[12] rasant verbreitet, welche eine noch höhere Abstraktion der darunterliegenden Infrastruktur ermöglichen. Unabhängig von der verwendeten Technologie muss der Cloud-Provider durch seine Architektur sicherstellen, dass zu keinem Zeitpunkt die Möglichkeit besteht, auf virtuelle Instanzen oder Prozesse eines anderen Anwenders zugreifen zu können.

---

[10] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 1: Introduction to the Cloud

[11] Xing, Yuping, and Yongzhao Zhan. "Virtualization and cloud computing." Future Wireless Networks and Information Systems. Springer, Berlin, Heidelberg, (2012): 308

[12] Bernstein, David. "Containers and cloud: From lxc to docker to kubernetes." *IEEE Cloud Computing* 1.3 (2014): 82

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Elastizität

  Ein wichtiges Kriterium für Cloud-Infrastrukturen ist die Elastizität. Abhängig von den Anforderungen eines Anwenders kann dieser dynamisch seine Ressourcen in der Cloud erweitern oder reduzieren.[13]

  Da Speicheranforderungen üblicherweise sehr stark wachsen, muss sich der Anwender nicht um die Erweiterung bzw. Beschaffung von neuer Hardware kümmern. Der Cloud-Provider bietet ihm eine Plattform, in der die darunterliegende Hardware transparent ist und für den Anwender jederzeit ausreichend Speicherkapazität zur Verfügung steht.[14] Sobald der Kunde die Daten nicht mehr benötigt, steht der freigegebene Speicher anderen Anwendern zur Verfügung. Die großen Cloud-Provider besitzen alle mehrere Exabytes an Speicherkapazität in den Rechenzentren, um die Anforderungen ihrer Anwender auf Elastizität jederzeit erfüllen zu können.

  Wird ein Web-Server in einer Cloud-Infrastruktur provisioniert, so kann dieser je nach Auslastung dynamisch skaliert werden. Gibt es mehr Zugriffe, werden zusätzliche Instanzen angefordert, wird die Anzahl der Zugriffe wieder geringer, können Instanzen heruntergefahren werden. Diese Elastizität muss durch die jeweilige Anwendung unterstützt werden. Die Cloud-Infrastruktur stellt die Ressourcen und die Möglichkeit zur Verfügung, dies umzusetzen.

- Kostenmodell

  Üblicherweise wird in der Cloud eine „pay what you use“ Verrechnung verwendet. Dies bedeutet, dass nur Ressourcen, die auch wirklich verwendet wurden, am Ende eines Monats verrechnet werden. Allgemein spricht man hier von einer Umwandlung von Investitionsausgaben (Capital Expenditure - CAPEX) in Betriebskosten (Operational Expenditure -

[13] Herbst, Nikolas Roman, Samuel Kounev, and Ralf Reussner. "Elasticity in cloud computing: What it is, and what it is not." 10th International Conference on Autonomic Computing ({ICAC} 13). (2013).

[14] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. “The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.” Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 1: Introduction to the Cloud

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

OPEX). Konkret werden Anschaffungskosten für Hardware, die in Unternehmen über längere Zeiten abgeschrieben werden müssen in operationale Kosten umgewandelt, welche für Unternehmen oft einfacher zu verwalten sind. Für die Berechnung der Kosten werden transparente Metriken verwendet die vom jeweils genützten Service abhängen.[15]

Betrachtet man den Speicher, so wird dieser üblicherweise in verwendeten Megabyte pro Tag abgerechnet. Wenn ein Anwender für 15 Tage 3 GB in der Cloud gespeichert hat, werden auch nur diese am Ende des Monates verrechnet. Zusätzlich können noch andere Metriken für die Bestimmung der Kosten verwendet werden. Ein Beispiel hierfür wäre die MB pro Monat, die durch den Cloud-Provider transferiert werden.[16]

Betrachtet man die Serverleistungen, so werden auch hier nur jene Ressourcen verrechnet, die auch tatsächlich verwendet wurden. Üblicherweise wird eine Instanz pro laufende Stunde oder Minute abgerechnet. Sehr häufig unterscheiden Cloud-Provider noch unterschiedliche Instanz Größen. Diese sind eine vorgefertigte Konfiguration einer virtuellen Maschine (CPU, RAM, Persistenter Datenspeicher, …).

Abhängig von Instanz Größe, Anzahl und Laufzeit werden die Kosten am Ende des Monats verrechnet.

2.2 Service-Modelle

Wie bereits vorhin erwähnt, gibt es unterschiedliche Modelle, um Cloud-Services zu kategorisieren. Eins der bekanntesten basiert auf der Abstraktion der Infrastruktur, die dem Anwender angeboten wird. Hierbei betrachtet man, welche Leistungen durch den Cloud-Provider und welche durch den Anwender ausgeführt werden.

---

[15] Talukder, Asoke K., and Lawrence Zimmerman. "Cloud economics: Principles, costs, and benefits." *Cloud computing*. Springer, London, (2010): 343-360.

[16] Becker, Steffen, Gunnar Brataas, and Sebastian Lehrig, eds. “Engineering Scalable, Elastic, and Cost-Efficient Cloud Computing Applications: The CloudScale Method. Springer, (2017): 11ff

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Abbildung 1 zeigt die weit verbreitete Unterteilung in Infrastruktur as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Diese werden in den nächsten Punkten näher betrachtet.[17]

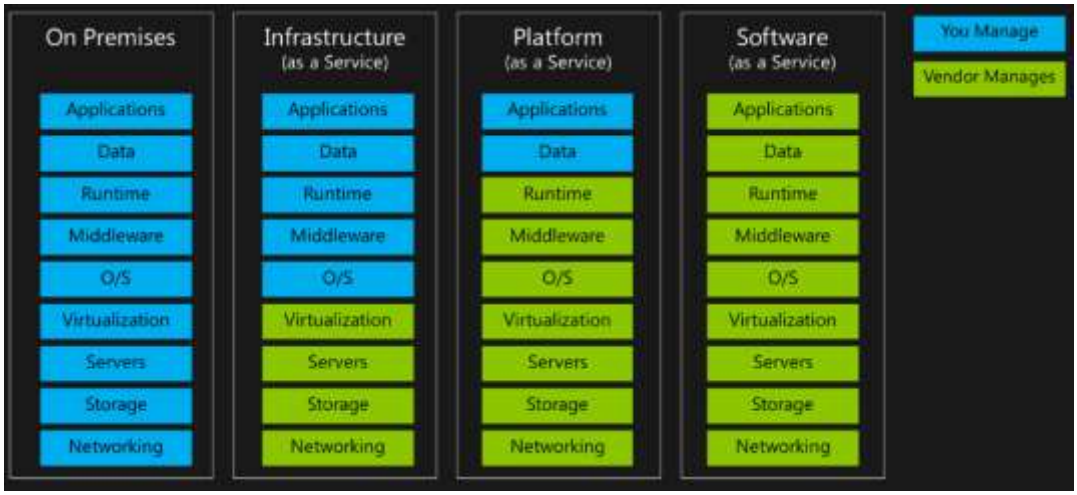

Abbildung 1: Einteilung von Cloud-Service-Modellen [18]

2.2.1 Infrastructure as a Service (IaaS)

IaaS bezeichnet neben SaaS das derzeit am weitesten verbreitete Service-Modell. Dieses Modell basiert auf der Möglichkeit, mittels Virtualisierung und Abstraktion, unterschiedliche Server auf einer gemeinsamen Hardware zu betreiben. Anwender müssen sich nicht mehr um das Beschaffen sowie den Betrieb von Hardware kümmern, sondern können sich auf den Betrieb und die Wartung von virtuellen Instanzen fokussieren. Sobald der Anwender eine virtuelle Maschine instanziiert hat, ist er für den logischen Betrieb dieser verantwortlich. Dies betrifft

[17] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 4: Cloud Service Models

[18] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 4: Cloud Service Models

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

im Speziellen die Installation sowie den Betrieb und Wartung des Betriebssystems und der Software.[19]

Aufgabenverteilung:

Cloud-Betreiber	Anwender
• Bereitstellung der virtualisierten Hardware • Sicherheit der Basisplattform	• Betrieb, Wartung und Updates des Betriebssystems • Betrieb, Wartung und Updates aller Softwarekomponenten • Sicherheit der virtuellen Maschine

Tabelle 1 IaaS Aufgabenverteilung

Vor- und Nachteile:

Vorteile	Nachteile
• Kaum Einschränkungen in Bezug auf die Software • Anwender kennen dieses Modell bereits • Einfache und schnelle Möglichkeit, die Vorteile der Cloud zu nutzen (Skalierung, „pay what you use“) • Nutzen von global verteilten Rechenzentren	• Geringes Einsparungspotential gegenüber klassischen Modellen • Hoher Wartungs- und Betriebsaufwand

Tabelle 2 IaaS Vor- und Nachteile

[19] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. “The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.” Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 4: Cloud Service Models

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

2.2.2 Platform as a Service (PaaS)

Plattform als Service beschreibt ein Modell, in dem der Cloud-Provider höherwertige Services zur Verfügung stellt. Beispiele wären Datenbanken, Messaging-Systeme, IoT, Benutzerverwaltung oder Autorisierung. In diesen Fällen stellt der Cloud-Provider die Services auf der Plattform zur Verfügung und gibt Anwendern die Möglichkeit diese in Applikationen zu integrieren. Die Integration passiert über APIs beziehungswiese standardisierte Protokolle, die es dem Anwender ermöglichen, Plattform-Komponenten auch auszutauschen. Generell ist festzustellen, dass eine Integration mit PaaS für den Anwender normalerwiese mit mehr Aufwand, meist sogar mit einer Änderung der bestehenden Applikation, verbunden ist. Dies bindet den Anwender stärker an den Cloud-Provider, bietet aber auch deutlich höhere Skalierungs- und Einsparpotentiale.[20]

Aufgabenverteilung:

Cloud-Betreiber	Anwender
• Betrieb der Plattformkomponenten • Skalierung der Plattformkomponenten • Betrieb, Wartung und Updates der Services • Sicherheit der Plattformkomponenten	• Integration der Plattformkomponenten in die Anwendung • Betrieb der Anwendung

Tabelle 3 PaaS Aufgabenverteilung

[20] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.“ Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 4: Cloud Service Models

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Vor- und Nachteile:

Vorteile	Nachteile
• Auslagerung von Betrieb und Wartung einiger Komponenten • Bessere Skalierbarkeit • Reduktion der laufenden Kosten	• Stärkere Bindung an den Cloud-Provider • Höherer Integrationsaufwand

Tabelle 4 PaaS Vor- und Nachteile

2.2.3 Software as a Service (SaaS)

Software als Service beschreibt ein Modell, in dem der Cloud-Provider Applikationen über eine Cloud-Infrastruktur zur Verfügung stellt. Diese Applikationen können von unterschiedlichen Anwendern verwendet werden. Meist ist der Zugriff auf die Applikation über einen Webbrowser oder eine API gegeben. In diesem Fall ist der Kunde nur für die Konfiguration, nicht jedoch für den Betrieb der Services verantwortlich. Die am bekanntesten und stärksten verbreiteten Beispiele für SaaS sind webbasierte E-Mail-Services wie O365 oder Google Apps/Gmail oder Datenbank als Service (DBaaS).[21] [22]

Aufgabenverteilung:

Cloud-Betreiber	Anwender
• Betrieb der Plattform • Skalierung der Anwendung	Konfiguration der Anwendung

[21] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.“ Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 4: Cloud Service Models

[22] Tang, Changlong, and Jiqiang Liu. "Selecting a trusted cloud service provider for your SaaS program." Computers & Security 50 (2015): 65

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

• Betrieb, Wartung und Updates aller Softwarekomponenten • Sicherheit der Anwendung	

Tabelle 5 SaaS Aufgabenverteilung

Vor- und Nachteile:

Vorteile	Nachteile
• Vollständige Auslagerung von Betrieb und Wartung der Applikation • Immer auf dem aktuellen Stand • Reduktion der Kosten	• Ein Standardservice für alle Benutzer • Geringe Kontrolle über den geografischen Ort der Daten

Tabelle 6 SaaS Vor- und Nachteile

2.3 Deployment-Modelle

Über die Jahre haben sich unterschiedliche Deployment-Modelle herausgestellt, die sich prinzipiell durch die Anzahl und Art der Anwender unterscheiden. Abhängig von diesen sind unterschiedliche Services mehr oder weniger relevant für das jeweilige Deployment-Modell.[23] In den Modellen wird zwischen je nach Typ der Anwender und der Lokalität der Cloud unterschieden. [24]

Unter On-premises versteht man eine Cloud, die lokal einem Unternehmen oder einer Organisation zugeordnet ist. Hierbei wird die Infrastruktur in den

[23] Vossen, Gottfried, Till Haselmann, and Thomas Hoeren. „Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte.“ Dpunkt. verlag, (2013): 75ff

[24] Cloud Security Alliance. „Security Guidance.“ https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf (zugegriffen: 1.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Räumlichkeiten des Kunden installiert und alle Services werden aus dieser bezogen.

Off-premises bezeichnet ein Modell, in dem die Ressourcen außerhalb der Räumlichkeiten des Kunden installiert sind. Hierbei hängt es von dem jeweiligen Betreiber ab, ob er den exakten Ort mit seinen Kunden teilt oder nicht.

2.3.1 Private Cloud

Bei diesem Modell wird eine Cloud für eine Organisation aufgebaut und dieser zur Verfügung gestellt. Innerhalb der Organisation können unterschiedliche Einheiten, Abteilungen oder Anwender auf die gemeinsame Infrastruktur zugreifen. Abhängig von den Anforderungen der Organisation kann die Infrastruktur erworben oder von einem anderen Unternehmen beigestellt werden. Es wird auch nicht näher definiert, wer für die Wartung und den Betrieb der Cloud zuständig ist. Dies kann entweder intern oder durch ein externes Unternehmen erfolgen. Für eine Private Cloud ist sowohl ein On-premises als auch ein Off-premises Modell möglich.[25]

Fast jedes Unternehmen verwendet in der Zwischenzeit Private Clouds um die Hardware besser zu benützten. Hierfür werden meist Virtualisierungstechnologien wie vmWare[26] Hyper-V[27] oder RedHat Virtualization[28] verwendet.

---

[25] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 3: Cloud Deployment Models

[26] „vmware". https://www.vmware.com/ (zugegriffen: 27.10.2020)

[27] Microsoft. „Hyper-V". https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v (zugegriffen: 27.10.2020)

[28] RedHat. „Enterprise Virtualization". https://www.redhat.com/en/technologies/virtualization/enterprise-virtualization (zugegriffen: 27.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

2.3.2 Community Cloud

In diesem Fall wird eine Cloud exklusiv für einen eingeschränkten Benutzerkreis aufgebaut und zur Verfügung gestellt. Meistens haben die Anwender einer Community Cloud gemeinsame Anforderungen (z.B.: Sicherheit, Compliance, Regulative, …) die einen Aufbau und Betrieb einer dedizierten Cloud für diese Gruppe sinnvoll und auch wirtschaftlich macht. Die Cloud kann durch eine der Organisationen oder durch ein externes Unternehmen besessen, betrieben und verwaltet werden.[29]

Ein gutes Beispiel sind sogenannte Government Clouds, die Unternehmen in Kooperation mit Regierungen bereitstellen. Meist werden diese Clouds als abgeschirmte Bereiche oder eigenständige Rechenzentren konzipiert, die nur durch speziell zertifizierte Personen betrieben und verwaltet werden. [30, 31]

2.3.3 Public Cloud

In diesem Modell stellt ein Unternehmen, eine Bildungseinrichtung oder eine öffentliche Organisation ihre Infrastruktur beliebigen Anwendern zur Verfügung. Es gibt kaum Einschränkungen, welche Anwender die Dienste verwenden können, solange sie mit dem Anbieter in eine Geschäftsbeziehung treten können. In einem oder mehreren Rechenzentren teilen sich Einzelpersonen sowie Großkunden die Infrastruktur. Die meisten Public Cloud-Provider haben Rechenzentren in unterschiedliche Regionen der Welt, um die Anforderungen an Datenlokation und Latenz ihrer Anwender umsetzen zu können. Durch die Skalierungsfaktoren entwickeln sich auch immer neue Services und die Kosten für Anwender können

---

[29] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 3: Cloud Deployment Models

[30] Microsoft. „Azure Government". https://azure.microsoft.com/en-us/global-infrastructure/government/ (zugegriffen: 27.10.2020)

[31] AWS. „AWS GovCloud (US)". https://aws.amazon.com/govcloud-us/ (zugegriffen: 27.19.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

geringgehalten werden. Dieses Modell ist heute sicher eines der am weitesten verbreiteten Cloud-Modelle.[32]

Beispiele für Public Clouds wären: Microsoft Azure[33], Microsoft Office 365[34], Amazon Web Services[35], Google Apps[36], Google Cloud[37] oder die SAP-Cloud Plattform[38].

2.3.4 Hybrid Cloud

Unter einer Hybrid Cloud versteht man den Zusammenschluss mehrerer der oben angeführten Modelle. Sehr häufig wird eine Private Cloud oder eine Community Cloud mit einer Public Cloud kombiniert. Die jeweiligen Cloud-Instanzen bleiben eigenständig, durch Standardisierung beziehungswiese die Benutzung von kompatibler Technologie in den unterschiedlichen Clouds können Anwender transparent auf die Instanzen zugreifen. Es gibt mehrere Anwendungsbereiche eines solchen Modelles.[39] [40]

- Cloud-Erweiterung

  Darunter versteht man die Möglichkeit, Services von einem Cloud-Provider zu beziehen, wenn die eigenen Ressourcen nicht mehr ausreichen.

---

[32] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 3: Cloud Deployment

[33] Microsoft. „Microsoft Azure". https://azure.microsoft.com/ (zugegriffen: 27.10.2020)

[34] Microsoft. „Office 365". https://www.office.com/ (zugegriffen: 27.1.2020)

[35] AWS. „Amazon Web Services AWS". https://aws.amazon.com/ (zugegriffen: 27.10.2020)

[36] Google. „Google Workspace". https://workspace.google.com/ (zugegriffen: 27.10.2020)

[37] Google. „Google Cloud". https://cloud.google.com/ (zugegriffen: 27.10.2020)

[38] SAP. „SAP-Cloud Platform". https://www.sap.com/products/cloud-platform.html (zugegriffen: 27.10.2020)

[39] Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. Cloud computing: Principles and paradigms. Vol. 87. John Wiley & Sons, (2010): Chapter 9)

[40] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice." Amsterdam: Syngress, an Imprint of Elsevier, (2014): Chapter 3: Cloud Deployment Models

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Regionale Reichweite

  Für viele Anwender ist es wichtig, Ressourcen so nahe wie möglich am Ort der Verarbeitung zu haben. Dies ist speziell in Szenarien relevant, wo es um schnelle Antwortzeiten (<100ms) geht oder, wenn Daten verpflichtend in einer Region gespeichert werden müssen (z.B. Finanzdaten). In diesem Modell können Anwender Infrastruktur eines Cloud-Providers benützen, wenn sie in dieser Region selbst keine Ressourcen besitzen. Sollten Anwender bereits einen Großteil ihrer Ressourcen in die Cloud ausgelagert haben, der Cloud-Provider in einer speziellen Region jedoch kein Rechenzentrum besitzen, kann der Anwender durch lokale Installationen die Cloud erweitern.

- Desaster

  Um für einen möglichen Ausfall in dem eigenen Rechenzentrum gerüstet zu sein, benützen viele Anwender einen Cloud-Provider, damit sie allenfalls ihre Ressourcen an einem anderen Ort weiter nutzen können.

Die meisten Public Cloud-Provider bieten in der Zwischenzeit auch hybride Lösungen an, da ihre Kunden sehr oft die Vorteile aus beiden Szenarien nutzen möchten. Beispiele hierfür sind: Azure Hybrid Cloud Solutions[41], Amazon Web Services[42] oder NetApp Hybrid Storage[43].

[41] Microsoft. „Azure Hybrid Cloud.“ https://azure.microsoft.com/en-us/solutions/hybrid-cloud-app/ (zugegriffen: 27.10.2020)
[42] AWS. „Hybrid Cloud.“ https://aws.amazon.com/hybrid/ (zugegriffen: 27.10.2020)
[43] NetApp. „Hybrid Cloud.“ https://www.netapp.com/hybrid-cloud/ (zugegriffen: 27.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

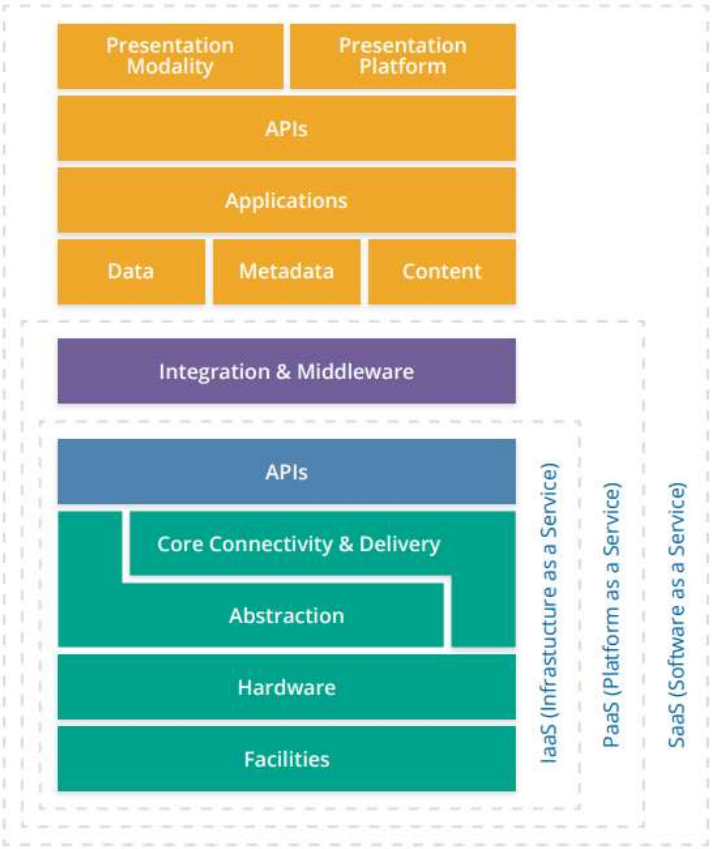

Abbildung 2: Referenz und Architektur Modell [44]

[44] Cloud Security Alliance. „Security Guidance“. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf (zugegriffen: 1.10.2020): S13

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 3
Rechtliche Betrachtung der Cloud

3.1 Zivil- und Vertragsrecht

3.1.1 Internationaler Charakter des Cloud-Vertrages, anwendbares Recht

Cloud-Services sind in der Regel grenzüberschreitende Sachverhalte, daher ist bei der Vertragsverfassung darauf zu achten, welches Recht zur Anwendung kommt. Das im EU-Rahmen anwendbare Recht ist bei vertraglichen Schuldverhältnissen grundsätzlich durch die Rom I Verordnung[45] geregelt.

Die Vertragsparteien können gemäß Art 3 Abs 1 Rom I Verordnung eine Rechtswahl treffen. In diesem Fall unterliegt der Vertrag dem von den Parteien gewählten Recht. Die Rechtswahl muss ausdrücklich erfolgen oder sich eindeutig aus den Bestimmungen des Vertrags beziehungsweise aus den Umständen des Falles ergeben. Die Parteien können eine Rechtswahl für den gesamten Vertrag oder nur für einen Teil treffen.[46]

Wenn die Vertragsparteien keine Rechtswahl treffen, bestimmt Art 4 Rom I Verordnung das anwendbare Recht. Bei den meisten in Frage kommenden Vertragstypen (z.B.: Dienstleistungsverträgen) kommt das Recht des Landes zur Anwendung, in dem die Partei, welche für den Vertrag charakteristische Leistungen zu erbringen hat, ihren gewöhnlichen Aufenthalt hat. Bei Cloud-

[45] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I)
[46] Art 3 Abs 1 Rom I

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Verträgen führt diese Regelung daher in den meisten Fällen zur Anwendung des am Sitz des Cloud-Anbieters anwendbaren Rechts.[47]

Bei unternehmensbezogenen Geschäften und standardisierten Verträgen wird in der Regel eine Rechtswahl getroffen.

Die Rom I Verordnung beschränkt die freie Rechtswahl, wenn ein Cloud-Anbieter einen Vertrag mit Verbrauchern abschließt. Hier ist das Recht des gewöhnlichen Aufenthaltsortes, des Konsumenten anzuwenden.[48]

3.1.2 Vertragstypologie und Vertragsmodelle

Die rechtlichen Grundlagen des Cloud Computing sind im Zivilrecht verankert, wobei die Einordnung des Cloud-Vertrages nicht ganz einfach ist. Die meisten Cloud-Verträge sind gemischte Verträge, in denen Elemente des Kauf-, Werk-, Dienstleistungs- und Mietvertrages enthalten sind.[49]

In Österreich gibt es weder Rechtsvorschriften noch Judikatur zur rechtlichen Einordnung des Cloud-Vertrages. Der Bundesgerichtshof (BGH) in Deutschland hat den Cloud-Vertrag als Mietvertrag klassifiziert, da oft eine entgeltliche Gewährung der Onlinenutzung vereinbart wird. Andere sehen in den Cloud-Verträgen Grundzüge des Dienst-, Werk- und Leihvertrages.[50] Die rechtliche Einstufung in Deutschland gründet sich auf das sogenannte ASP-Urteil[51], das die entgeltliche, zeitlich befristete Nutzung einer auf dem Server des Anbieters laufenden Software über das Internet (oder andere elektronische Netze) sowie die Zurverfügungstellung von Speicherkapazität als Miete qualifiziert hat.[52]

---

[47] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag, (2011): 45-46

[48] Art 6 Rom I

[49] Michael Rohrlich. „Cloud Computing - Rechtliche Grundlagen.“ Rechtliche Grundlagen, entwickler.press 2014: 2.1 Zivilrechtliche Grundlagen

[50] Michael Rohrlich. „Cloud Computing - Rechtliche Grundlagen.“ Rechtliche Grundlagen, entwickler.press 2014: 2.2 Besonderheiten im IT-Recht

[51] BGH, Urteil vom 15.11.2006, Az. XII ZR 120/04 = MMR 2007, 243 ff.

[52] Kompetenzzentrum Trusted Cloud. „Leitfaden – Vertragsgestaltung beim Cloud Computing Nr 3.“ https://www.trusted-cloud.de/sites/default/files/ap_3_vertragsleitfaden.pdf (zugegriffen: 01.06.2020): 33

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Aufgrund der Ähnlichkeiten zwischen dem österreichischen und deutschen Recht geht *Marko* in Österreich auch von einer Einordung unter das Mietrecht aus und sieht dafür Anhaltspunkte in der OGH-Entscheidung 6 Ob 69/05y. In dieser wurde ein Mobilfunkvertrag nicht als Werkvertrag, sondern als Mischvertrag mit dienstvertraglichen und mietvertraglichen Elementen eingestuft.[53]

Je nach Ausgestaltung der Vertragsbeziehungen zwischen Cloud-Nutzer und Cloud-Provider gibt es verschiedene Vertragsmodelle. Abhängig davon, ob die Dienstleistungen von einem oder von mehreren Anbietern bezogen werden, kann man zwischen *single-vendor* und *multi-vendor*-Modell unterscheiden. Beim multi-vendor-Modell gibt es Unterschiede, ob die Cloud-Nutzer die verschiedenen Anbieter selbst verwalten oder diesen Aufwand bei einem Generalunternehmer ausgelagert ist. Beim Generalunternehmer gibt es den Vorteil, dass dieser gegenüber dem Nutzer direkter Ansprechpartner ist und für den Subunternehmer gemäß § 1313 a ABGB im Wege der Gehilfenhaftung einzustehen hat.[54]

3.1.3 Gewährleistung und Haftung

3.1.3.1 Gewährleistung

Im österreichischen Recht ist die vertragliche Gewährleistung in den §§ 922ff ABGB geregelt und bestimmt die Haftung für eine mangelhaft erbrachte Leistung. Unter Mangel versteht man ein Abweichen der erbrachten Leistung von den vertraglich vereinbarten oder üblicherweise vorausgesetzten Eigenschaften.[55]

§ 932 ABGB nennt als Rechtsbehelfe die Verbesserung, Austausch, Preisminderung und Wandlung, wobei die ersten zwei primäre, und die letzten zwei sekundäre Gewährleistungsbehelfe sind. Die Verbesserung und der

[53] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag, (2011): 30

[54] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag, (2011): 26-29

[55] Wirtschaftsagentur Wien (Hrsg: Paul Meinl). „Software as a service, Verträge richtig abschließen.“ 2 Aufl., http://www.it-lab.at/__docs/SaaS-Leitfaden__31.pdf (zugegriffen: 6.10.2019): 28

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Austausch sind in angemessener Frist und möglichst mit geringen Unannehmlichkeiten für den Übernehmer durchzuführen. Ist dies unmöglich oder mit unverhältnismäßig hohem Aufwand für den Übergeber verbunden, kommen Preisminderung oder Wandlung in Frage. Eine Wandlung ist nur möglich, wenn der Mangel nicht geringfügig ist.[56]

Aufgrund der Einordnung von Cloud-Verträgen als Mietvertrag folgt die gesetzliche Verpflichtung des Cloud-Providers nach § 1096 ABGB, den Bestandgegenstand in brauchbarem Zustand zu erhalten und den Cloud Nutzer im Gebrauch nicht zu stören.[57] Bei den Bestandverträgen handelt es sich um Dauerschuldverhältnisse, bei denen Gebrauchsüberlassung geschuldet ist. Eine Nachholung ist nur in den seltensten Fällen möglich, daher können die primären Gewährleistungsbehelfe Verbesserung oder Austausch gemäß §§ 922ff ABGB nicht angewendet werden.[58] Es kommt daher die verschuldensunabhängige Sondergewährleistungsbestimmung oder Mietzinsminderung nach § 1096 ABGB zur Anwendung.[59] Bei Nichterfüllung ist der Bestandnehmer daher ganz oder teilweise von seiner Pflicht zur Zahlung zu befreien.[60] Eine Zinsminderung in Verbraucherverträgen ist nicht zulässig, weil dies gegen § 9 KSchG verstoßen würde.[61, 62] Der Bestandnehmer muss sich nicht mit der Zahlungsminderung begnügen, sondern kann auch die Vertragserfüllung und Unterlassung von Störungen einfordern oder den Vertrag auflösen.[63] Gemäß § 1117 ABGB ist der Bestandnehmer berechtigt, auch vor Verlauf der vereinbarten Zeit von dem Vertrag ohne Kündigung zurückzutreten, wenn das Bestandstück in einem Zustand übergeben oder ohne seine Schuld in einen Zustand geraten ist, der es zu dem vereinbarten Gebrauch untauglich macht. Dies gilt auch wenn ein beträchtlicher Teil durch Zufall auf eine längere Zeit entzogen oder unbrauchbar wird (z.B.: Ausfall der Cloudleistung).

---

[56] Welser/Zöchling-Jud, Bürgerliches Recht II, (2015): Rz 333-338

[57] Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 43

[58] Riss in Kletečka/Schauer, ABGB-ON1.02 § 1096 (Stand 1.10.2016. rdb.at): Rz 24-25

[59] Riss in Kletečka/Schauer, ABGB-ON1.02 § 1096 (Stand 1.10.2016, rdb.at): Rz 24-25

[60] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 999

[61] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 999

[62] Riss in Kletečka/Schauer, ABGB-ON1.21 § 1096 (Stand 1.10.2016, rdb.at): Rz 27

[63] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1000

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

In den Cloud-Verträgen werden oft Gewährleistungs- und Haftungsbeschränkungen getroffen. Hierbei ist eine detaillierte Beschreibung einzelner Leistungen und insbesondere der Cloud-spezifischen Aspekte sehr wichtig. In so genannten Service Level Agreements (SLA) werden üblicherweise die Standards der Leistungserbringung festgelegt.[64] Zum Inhalt des Cloud Vertrags siehe 3.1.3.5.

3.1.3.2 Sorgfaltspflichten des Cloud-Providers

Im österreichischen Zivilrecht unterliegt der Cloud-Provider als Sachverständiger einem objektivierten Sorgfaltsmaßstab.[65] Für Sachverständige gilt ein strengerer Maßstab, sie müssen durchschnittliche Fähigkeiten ihres Berufsstandes haben.[66] Der Cloud-Provider ist verpflichtet, seine Cloud auf Basis einer Sicherheitsarchitektur zu implementieren und zu betreiben, die dem typischen Standards entspricht.[67] Eine Darstellung der weltweit geltenden Standards findet sich in Kapitel 3.3 Standards und Frameworks.

3.1.3.3 Haftung des Cloud Dienstleisters gegenüber seinen Kunden

Neben der Pflicht, die vertragliche Leistung zu erbringen, kann der Cloud-Provider gegenüber seinen Kunden schadenersatzpflichtig werden. Es handelt sich hier nicht um Fälle der Nichtverfügbarkeit der Dienstleistungen (diese wurden im Punkt 3.1.3.1 Gewährleistung behandelt), sondern um anders entstandene Schadensfälle, für die der Cloud-Provider bei Erfüllung folgender Voraussetzungen haftet:

---

[64] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 34-35

[65] R. Blaha-R. Makro-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 103

[66] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1517

[67] R. Blaha-R. Makro-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 103

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Schaden

  Voraussetzung für die Durchsetzung eines Schadenersatzanspruchs ist der Eintritt eines tatsächlichen Schadens. Schaden heißt jeder Nachteil, welcher jemanden an Vermögen, Rechten oder seiner Person zugefügt worden ist. Davon unterscheidet sich der Gewinnentgang, den jemand nach dem gewöhnlichen Laufe der Dinge zu erwarten hatte.[68] Die Literatur unterscheidet zwischen dem **positiven Schaden** (hier handelt es sich im Wesentlichem um die Beschädigung oder Zerstörung eines schon vorhandenen Gutes) und **dem entgangenen Gewinn** (wenn eine Vermögensvermehrung vermindert, also die Erwerbschance verhindert wird).[69]

  In der Cloud können zahlreiche Schadensfälle eintreten. Meiner Meinung nach entsteht ein positiver Schaden, wenn z.B.: Daten oder Software des Cloud-Nutzers gestohlen oder unwiederbringlich gelöscht werden. Entgangener Gewinn könnte in Betracht kommen, wenn der Cloud-Nutzer selbst Unternehmer ist, seine Dienstleistungen über die Cloud-Plattform zur Verfügung stellt und diese aufgrund einer Störung der Dienste nicht erbringen kann.

  Positiver Schaden und entgangener Gewinn bilden zusammen das **Interesse**. Der Verschuldensgrad des Schädigers bestimmt, ob beides ersetzt werden muss.[70]

- Verursachung durch den Cloud-Provider

  Hier ist im Hinblick auf die Kausalität zu prüfen, ob der Cloud-Provider den Schaden durch eigenes Verhalten (Handlung oder Unterlassung) verursacht hat, oder ob Personen oder Sachen, für die er einstehen muss, verantwortlich waren.[71] Beim Cloud-Vertrag kommt meist Unterlassung in Frage, z.B. wegen unterlassene Maßnahmen betreffend Netzsicherheit oder

[68] § 1293 ABGB
[69] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1349
[70] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1351
[71] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1365

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Virenschutz.[72] Wichtig hierbei ist, dass eine Unterlassung nur ursächlich ist, wenn ein entsprechendes positives Verhalten den eingetretenen Schaden vermieden hätte.[73]

- Rechtswidrigkeit

  Ein kausal verursachter Schaden ist dann schadenersatzrechtlich relevant, wenn dieser rechtswidrig herbeigeführt wurde. Bei der Vertragshaftung besteht die Rechtswidrigkeit bereits in der Nichterfüllung der vor- oder nachvertraglichen Pflichten.[74] *Blaha* qualifiziert die oben genannten Beispiele (Virenschutz nicht auf dem aktuellen Stand, Datenverkehr nicht verschlüsselt und nicht gesichert), als rechtswidrige Verletzung von Vertragspflichten des Cloud-Providers, auch dann, wenn sie im Vertrag nicht ausdrücklich vereinbart wurden.[75]

- Verschulden

  Verschulden bedeutet die Vorwerfbarkeit eines rechtswidrigen Verhaltens.[76] Der Ersatz des Schadens richtet sich nach dem Grad des Verschuldens des Schädigers. Bei leichtem Verschulden ist nur der positive Schaden zu ersetzen, bei Vorsatz oder grober Fahrlässigkeit ist volle Genugtuung zu leisten.[77] In diesem Fall wäre daher auch der entgangene Gewinn des Cloud-Nutzers, den er durch Ausfall der Dienstleistung erleidet, zu ersetzen.

  Wie bereits im Punkt 3.1.3.2 erwähnt, haften der Cloud-Provider und seine Erfüllungsgehilfen (z.B: Mitarbeiter oder Subunternehmer) als Sachverständige für die Erbringung der Leistung, wobei sie über

[72] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. Rechtsfragen des Cloud Computing, Medien und Recht Verlag, 2011 S 106

[73] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1365

[74] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1390

[75] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 107

[76] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1412

[77] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015): Rz 1432-1435

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Fähigkeiten und Kenntnisse eines typischen Cloud-Providers verfügen müssen. *Blaha* sieht ein grobes Verschulden des Cloud-Providers darin, wenn z.B. seine Erfüllungsgehilfen ungenügende Kenntnisse für die Abwehr von Malware-Bedrohungen oder die Erstellung von Backups verfügen. Ein einmaliges Übersehen eines sicherheitsrelevanten Patches qualifiziert er als leichte Fahrlässigkeit.[78]

3.1.3.4 Grenzen der Vertragsgestaltung und Haftungsbeschränkung

In der Praxis bieten Cloud-Provider ihre Services im Rahmen von Allgemeinen Geschäftsbedingungen an, weil sie die Bestimmungen des Vertrages nicht mit den Kunden einzeln verhandeln wollen. Zentrale Frage bei einem Vertragsabschluss ist die Regelung der Haftungsbeschränkung, wobei die meisten Verträge diesbezüglich einen Höchstbetrag festlegen. Es stellt sich die Frage, in welchem Ausmaß die Haftungsbeschränkung nach dem österreichischen Recht zulässig ist.

Ein Haftungsausschluss für vorsätzliche Schadenszufügung ist jedenfalls sittenwidrig und daher unwirksam. Der Ausschluss der Haftung für grobe Fahrlässigkeit ist dann unzulässig, wenn er sittenwidrig ist. Dies ist der Fall, wenn die Fahrlässigkeit so extrem ist, dass mit einem derartigen Verhalten nach den Erfahrungen des täglichen Lebens und nach redlicher Verkehrsausübung, nicht gerechnet werden kann. Der Umstand, dass eine Klausel sittenwidrig ist, führt nicht unmittelbar zum Entfall dieser Vertragsklausel, sondern nur zu deren geltungserhaltenden Reduktion auf den rechtlich erlaubten Inhalt. Die Haftung für leichte Fahrlässigkeit kann grundsätzlich ausgeschlossen werden.[79]

Im Hinblick auf die obigen Ausführungen würde ich eine grobe Fahrlässigkeit sehen, wenn Anwender Daten verlieren, weil der Cloud-Provider eine ihm zur Kenntnis gelangte Sicherheitslücke nicht rechtzeitig durch ein Update schließt, oder wenn er für SaaS-Anwendungen keine ausreichenden technischen und

[78] R. Blaha-R. Makro-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 108

[79] R. Blaha-R. Makro-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag (2011): 111

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

organisatorischen Rahmenbedingungen schafft, damit ein Datenverlust ausgeschlossen werden kann.

3.1.3.5 Wichtige Klauseln im Cloud-Vertrag

Der Abschluss eines Cloud-Vertrages bringt verschiedene Risiken mit sich. Es handelt sich hier einerseits um technische (z.B.: Vertraulichkeit und Verfügbarkeit der Daten) und andererseits auch um wirtschaftliche Risiken (z.B. Verlust von Daten, die in der Cloud gespeichert wurden).

Um die Risken zu vermeiden bzw. allfällige Schäden zu minimieren, ist es zu empfehlen, im Cloud-Vertrag folgende Punkte zu definieren: [80]

- **Vertragsparteien**

  Genaue Bezeichnung der natürlichen und/oder juristischen Personen, die den Vertrag abschließen.

- **Rechtswahl**

  Cloud-Verträge werden in der Regel grenzüberschreitend abgeschlossen. Um sich die allenfalls mühsame Ermittlung des anwendbaren Rechts zu ersparen, sollte beim Vertragsabschluss das anwendbare Recht festgelegt werden.

  Musterklausel:

  „German law applies. The application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is not permitted. "[81]

[80] Kompetenzzentrum Trusted Cloud. „Leitfaden – Vertragsgestaltung beim Cloud Computing Nr 3." https://www.trusted-cloud.de/sites/default/files/ap_3_vertragsleitfaden.pdf (zugegriffen: 01.06.2020): S 18-19, 32-33

[81] Cloudiax. „Contract terms for licensing of cloud services." https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 17.2

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- **Gerichtsstand**

  Ein wichtiger Vertragsbestandteil ist die Vereinbarung des Gerichtsstandes. Nähere Erläuterungen dazu siehe Kapitel 3.1.1.

  Musterklausel:

"The place of jurisdiction is the domicile of the Provider. The Provider can also sue the Customer in whose domicile."[82]

- **Vertragsbeginn**, **Vertragsende**, sowie **Kündigungsmöglichkeiten**

  Musterklausel:

"The term of contract shall begin with the submission of the access data for the cloud service to the Customer. The term of the Contract shall be one year, if no other term is accepted in the order confirmation by the Provider and shall be extended automatically by one year unless one of the parties has not terminated the Contract at least one month before the end of the contract term.

Furthermore, the contract is also terminated, if the Customer does not meet the payment obligation before the start of the contract renewal.

Furthermore, both the Provider and the Customer shall be able to terminate the contract due to important reasons without notice."[83]

- Zulässigkeit von **Subunternehmerleistungen**

[82] Cloudiax. „Contract terms for licensing of cloud services."
https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 17.5
[83] Cloudiax. „Contract terms for licensing of cloud services."
https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 6.1.-6.3.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Es soll geregelt werden, ob der Cloud-Provider einen Subunternehmer einsetzen darf. Wie bereits im Punkt 3.1.2 dargestellt, haftet der Cloud-Provider für die Leistung seines Erfüllungsgehilfen.

Musterklausel:

"The Provider is free to use subcontractors to fulfill its obligations. The Customer already declares his consent to this. A list of subcontractors is available at ...."[84]

- **Leistungsbeschreibung**

  Diese umfasst die genaue Beschreibung der Leistungen, insbesondere im Rahmen von Service Level Agreements (SLA), die die Qualität der Dienstleistung und die Rechtsfolgen bei Nichterfüllung oder Schlechterfüllung festlegen. Die SLAs sollten insbesondere folgende Punkte erfassen:

  - detaillierte Regelung der **Verfügbarkeit**

    Wichtig ist hier, den Bezugspunkt des Service Levels genau zu definieren. Als Bezugspunkt wird meist der Eingangspunkt des Cloud-Providers definiert, da er nicht für Ausfälle außerhalb seines Zuständigkeitsbereiches verantwortlich gemacht werden möchte. Dies kann aber dazu führen, dass die Verfügbarkeit für den Cloud-Provider gegeben ist, obwohl der Anwender die Leistung nicht beziehen kann. Die Verfügbarkeit einer Cloud-Leistung wird üblicherweise als Prozentwert in Bezug auf einen bestimmten Betrachtungszeitraum angegeben, z. B. „99,5 % im Monat". Darüber hinaus sollte klargestellt werden, welche Fälle nicht als Ausfall gewertet werden. [85]

[84] Cloudiax. „Contract terms for licensing of cloud services." https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 9.

[85] Cloudiax. „Contract terms for licensing of cloud services." https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 37.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Regelung der **Entstörzeiten**

  Hier ist zu bestimmen, ob der Cloud-Anbieter jede Störung des Cloud-Dienstes innerhalb eines fest definierten Zeitfensters zu beheben hat (sog. „Time to Repair“ oder „TTR“), ob eine durchschnittliche Entstörzeit für alle Störungen innerhalb eines definierten Zeitraumes gelten soll (oft als „Mean Time to Repair“ oder „MTTR“ bezeichnet) oder ob stattdessen nur Reaktionszeiten geschuldet sind. Meist werden in den Verträgen Reaktionszeiten vereinbart, in denen der Cloud-Provider den Anwender über das Vorhandensein einer Störung informiert.[86]

- Rechtsfolgen der **Schlechtleistung**

  Es werden pauschale Minderungsbeiträge für das zu zahlende Entgelt vereinbart. Diese werden auch “Service Credits” genannt. Häufig werden diese Service Credits gegen den zu erbringenden Rechnungsbetrag gegengerechnet.[87]

- **Vertragsstrafen**

  In dieser verspricht der Anbieter dem Kunden die Zahlung eines Geldbetrages für Nicht- oder Schlechterfüllung.[88]

Musterklausel:

“Service Level:

The Provider shall provide the cloud service with an availability of 99,5 % within the operational period. The operational period is 24 hours on 365 days a year and 366 days on leap-years. Except of the following maintenance windows which shall not be deemed as a period of operation and shall not be included in the calculation of availability.

---

[86] Cloudiax. „Contract terms for licensing of cloud services.“ https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 38.
[87] Cloudiax. „Contract terms for licensing of cloud services.“ https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 39.
[88] Cloudiax. „Contract terms for licensing of cloud services.“ https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkt 40.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Every first Sunday a month from 00:00 to 04:00 CET/CEST. This is a general maintenance window.

One hour per week for the Customer individual systems. This maintenance window shall be determined by the Customer before go live.

Any maintenance window for maintenance work which could not be postponed as long as the Provider has informed the Customer at least one week in advance. The information is provided on the status page https://status.cloudiax.com.

Availability shall be measured and calculated based on a calendar month. Availability shall be calculated using the following formula:

$$Value\ in\ percent = \frac{\Sigma\ Downtime\ during\ the\ operational\ period}{\Sigma\ \text{Service time} - \Sigma\ \text{Excused downtime}} \times 100$$

...

General liability of the provider:

The Provider shall be liable to the Customer (1) for damages he or his legal representatives or assistants have caused either purposely or by culpable negligence, and (2) for damages deriving from the loss of life, bodily injury or harm to health that the Provider, his legal representatives or vicarious agents are responsible for.

The Provider shall not be liable in the case of slight negligence, unless it has breached an essential contractual obligation, whose fulfilment enables the proper implementation of the contract and whose observance is regularly trusted and should be presumable by the Customer. This liability shall be limited to damages that are foreseeable and typical of the contract, this shall also apply to lost profit and cost savings failing to occur. Liability for other remote subsequent damage is excluded. For a single claim, the liability shall

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

be limited to the contractual value and in the case of current payments to the value for one contractual month.'[89]

- Vertragliche Regelung von **Gewährleistung** und **Haftung** unter Berücksichtigung der zulässigen Beschränkungen.

- Vereinbarungen zu **Geheimhaltung, Datensicherheit** und **Datenschutz** inklusive Regelung der Sanktionen bei Verstößen und Vereinbarung eines einheitlich hohen Datenschutzniveaus.

3.2 Datenschutzrecht

Primär ist der Datenschutz national und auf europäischer Ebene geregelt. Darüber hinaus gibt es einige internationale Abkommen.

3.2.1 Internationaler Datenschutz

Einige der wichtigsten internationalen Organisationen haben bereits sehr früh die Wichtigkeit der Selbstbestimmung über personenbezogene Daten erkannt und versucht diese zu regeln.

- Vereinte Nationen

  Bereits in der Allgemeinen Erklärung der Menschenrechte, die am 10. Dezember 1948 von der Generalversammlung der Vereinten Nationen ratifiziert wurde, misst man der Privatsphäre im Art. 12 der Menschenrechtserklärung Bedeutung zu. In dieser heißt es:

„Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr […] ausgesetzt werden. Jeder hat

[89] Cloudiax. „Contract terms for licensing of cloud services.“ https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020): Punkte 3. und 13

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“[90]

Die Erklärung ist für die ratifizierenden Staaten nicht verbindlich, kann jedoch als erster Versuch eines supranationalen Datenschutzes gesehen werden.

Auf dieser Basis versuchen seither mehrere Länder und Organisationen, das Recht auf Privatsphäre und Datenschutz als Menschenrecht inhaltlich weiter zu definieren.

- OECD

  Im Jahr 1980 stellte die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) Leitlinien für den Schutz des Persönlichkeitsbereiches auf. Primär wollte die Organisation den grenzüberschreitenden Austausch von personenbezogenen Daten erleichtern. Heute haben die OECD Empfehlungen keine praktische Bedeutung, da sie in der Zwischenzeit inhaltlich überholt und nicht auf die neuen Anforderungen des Internets ausgelegt sind.[91]

- Europäische Union

  Die Charta der Grundrechte der Europäischen Union wurde im Jahr 2000 von den Staats- und Regierungschefs der EU-Mitgliedsstaaten ratifiziert. Im Art. 7 der Charta wird das Recht auf Achtung des Privat- und Familienlebens, ihrer Wohnung sowie der Kommunikation verankert. Art. 8 ergänzt dies mit einem Recht auf personenbezogene Daten. Durch den Vertrag von Lissabon wurde die Charta durch alle EU-Mitgliedsstaaten

[90] UNO „Resolution der Generalversammlung 217 A(III). Allgemeine Erklärung der Menschenrechte“. https://www.un.org/Depts/german/menschenrechte/aemr.pdf (zugegriffen: 20.10.2020)

[91] OECD „Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten“. http://www.oecd.org/digital/ieconomy/15589558.pdf (zugegriffen: 20.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

ratifiziert und verankert damit den Datenschutz als Grundrecht für alle EU-Bürger.[92]

Die neue Rechtsgrundlage für Datenschutzrecht in der Europäischen Union ist die Datenschutz-Grundverordnung (DSGVO, DS-GVO oder GDPR)[93] welche im Kapitel 4.1.1.3 Datenschutz-Grundverordnung (DSGVO) im Detail behandelt wird.

- Europarat

  Die Europäische Menschenrechtskonvention wurde 1950 unterzeichnet und trat 1953 in Kraft. Gemäß Art. 8 Abs. 1 der Konvention hat

„jedermann […] Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs“.[94]

Nachdem der elektronische Datenaustausch in den 1970er Jahren immer wichtiger wurde, schaffte der Europarat 1980 ein Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten, welches 1985 in Kraft trat. In der Europäischen Datenschutzkonvention, wie das Übereinkommen auch genannt wird, verpflichten sich die unterzeichnenden Staaten, gewisse Grundprinzipien des Datenschutzes zu beachten und diese auch gegenüber Drittstaaten durchzusetzen.

Wie bereits erwähnt ist der Datenschutz national geregelt, viele international operierenden Unternehmen müssen aber auf die lokalen Datenschutz Rechte Rücksicht nehmen. Die folgende Abbildung gibt eine Übersicht, wie stark der Schutz in den jeweiligen Ländern der Welt geregelt ist und umgesetzt wird.

---

[92] Europäische Union. “Charta der Grundrechte der Europäischen Union.“ 2000/C 364/01. https://www.europarl.europa.eu/charter/pdf/text_de.pdf (zugegriffen: 20.10.2020)

[93] Europäisches Parlament und Rat. VERORDNUNG (EU) 2016/679 (Datenschutz-Grundverordnung) DSGVO. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 (zugegriffen: 10.10.2020)

[94] Europarat. “Die Europäische Menschenrechtskonvention.“ https://www.echr.coe.int/Documents/Convention_deu.pdf (zugegriffen: 20.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

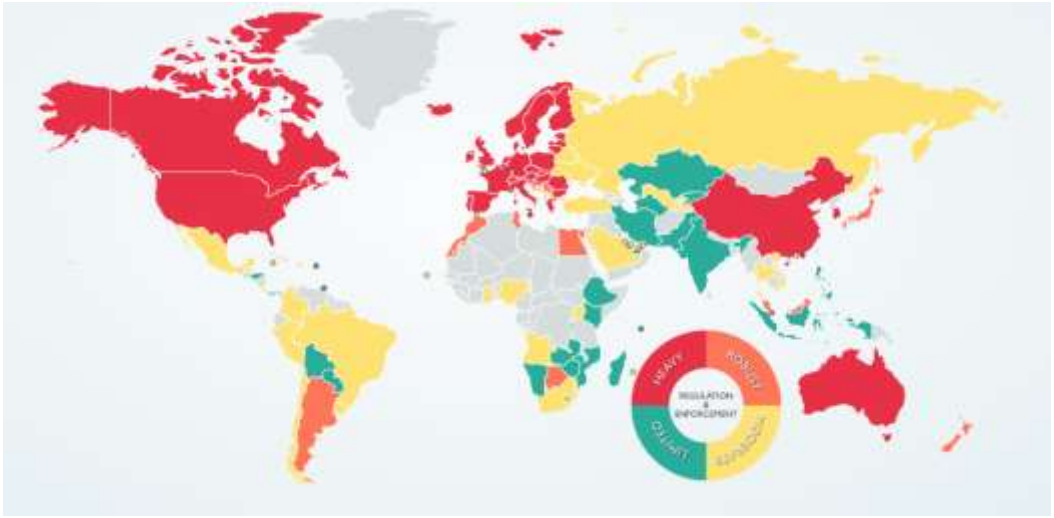

Abbildung 3: Übersicht des Datenschutzes Weltweit [95]

3.2.2 Datenschutzrechtliche Stellung des Cloud Anbieters

Aus datenschutzrechtlicher Sicht sind beim Cloud Computing folgende drei Rollen zu beachten:

- **Betroffene Person**

  Die betroffene Person ist gemäß Art 4 Abs 1 erster Halbsatz DSGVO eine identifizierte oder identifizierbare natürliche Person.

- **Verantwortlicher**

  Darunter versteht man nach Art 4 Z 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten

[95] DLA PIPER. „Data Protection Laws of the world." https://www.dlapiperdataprotection.com/ (zugegriffen: 29.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

geregelt, so kann der Verantwortliche beziehungsweise können bestimmten Kriterien seiner Benennung vorgesehen werden.

- **Auftragsverarbeiter**[96]

  Kann gemäß Art 4 Z 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Die Rollenverteilung im Datenschutzrecht ist für jede Verarbeitungstätigkeit gesondert zu beurteilen. Im Fall einer Datenverarbeitungstätigkeit stehen zunächst der Verantwortliche und die betroffene Person gegenüber. Bei Datenübermittlungen tritt auch jeder Dritte als Adressat in Erscheinung.[97]

Unter **Verarbeitung** versteht man das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung im Zusammenhang mit personenbezogenen. Diese Tätigkeiten können mit oder ohne Hilfe automatisierter Verfahren ausgeführten werden.[98]

Der Cloud-Provider übernimmt in dieser Rollenverteilung die Stellung des Auftragsverarbeiters, der Cloud-Nutzer die Stellung des Verantwortlichen. Sie schließen miteinander in der Regel einen zivilrechtlichen Vertrag ab.

Der Auftragsverarbeiter darf personenbezogene Daten nur auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments ausschließlich für die Zwecke des Verantwortlichen verarbeiten. Wenn der Auftragsverarbeiter dagegen verstößt und Zwecke und Mittel der Datenverarbeitung selbst bestimmt, gilt er selbst als Verantwortlicher.[99, 100]

---

[96] Bergauer/Jahnel/Mader/Staudegger (Hrsg). „jusIT Spezial: DS-GVO.“ LexisNexis (2018): 31
[97] Bergauer/Jahnel/Mader/Staudegger (Hrsg). „jusIT Spezial: DS-GVO.“ LexisNexis (2018): 31
[98] Art 4 Z 2 DSGVO
[99] Art 28 Abs 10 DSGVO
[100] Bergauer/Jahnel/Mader/Staudegger (Hrsg). „jusIT Spezial: DS-GVO.“ LexisNexis (2018): 36

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3.2.3 Rechtliche Anforderungen

3.2.3.1 Zulässige Datenverarbeitung durch den Auftraggeber

Hier hat der Verantwortliche die folgende Datenschutzgrundsätze und die Rechtmäßigkeit der Verarbeitung zu beachten:[101]

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit.

Diese Grundsätze werden in Art. 5 Abs 2 durch den neuen Grundsatz der Rechenschaftspflicht ergänzt.[102] Nach Abs 2 ist der Verantwortliche für die Einhaltung des Abs 1 verantwortlich und muss dessen Einhaltung nachweisen können. Dieser Grundsatz macht es erforderlich, dass ein Unternehmen aktiv Compliance-Maßnahmen implementiert, welche die Einhaltung der oben genannten Grundsätze sicherstellen und die Einhaltung dieser Grundsätze auch nachweisen kann.[103]

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

> *„(a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;*

[101] Art 5 und 6 DSGVO
[102] Bergauer/Jahnel/Mader/Staudegger (Hrsg). „jusIT Spezial: DS-GVO.“ LexisNexis (2018): 56
[103] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018): 11

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

(b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

(c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

(d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

(e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

(f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.[104]

3.2.3.2 Sorgfältige Auswahl des Cloud-Providers

Wenn eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, so darf dieser nur mit Auftragsverarbeitern arbeiten, die hinreichend Garantien bezüglich geeigneter technischer und organisatorischer Maßnahmen liefern. Diese Garantien müssen gewährleisten, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.[105]

Die Verarbeitung durch einen Auftragsverarbeiter darf nur auf Grundlage eines schriftlichen Vertrags erfolgen, der auch elektronisch umgesetzt werden kann.[106] Der erforderliche Inhalt des Vertrages ist in Art 28 Abs 3 lit a) bis f) DSGVO

[104] Art 6 Abs 1 DSGVO
[105] Art 28 Abs 1 DSGVO
[106] Art 28 Abs 3 und 9 DSGVO

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

festgelegt. Die DSGVO stellt aber keine abschließende, sondern nur eine exemplarische Aufzählung dar.

Ein Auftragsverarbeiter, der gegen die DSGVO verstößt und die Zwecke und Mittel der Verarbeitung selbst bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.[107]

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien nachzuweisen.[108]

3.2.3.3 Erfüllung Datensicherheitsmaßnahmen

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

diese Maßnahmen schließen unter anderem Folgendes ein:

(a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

(b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

(c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

[107] Art 28 Abs 10 DSGVO
[108] Art 28 Abs 5 DSGVO

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

(d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“[109]

Nach der DSGVO hat der Verantwortliche und der Auftragsverarbeiter ein dem Risiko angemessenes Schutzniveaus zu gewährleisten. Wie hoch das Risiko ist, hängt von den Kategorien der zu verarbeitenden Daten und von den Verarbeitungszwecken ab.[110]

Um zu prüfen, ob das Sicherheitsniveau tatsächlich ausreichend ist, ist eine detaillierte Risikoanalyse erforderlich. In der Praxis orientiert man sich an Best Practices oder technischen Standards.[111]

3.2.3.4 Stellung des Subdienstleisters

Ein Auftragsverarbeiter darf grundsätzlich nur mit Genehmigung des Verantwortlichen einen Sub-Auftragsverarbeiter einsetzen; dies kann entweder durch eine konkrete Genehmigung für den Einzelfall oder durch eine Generalgenehmigung mit Widerspruchsmöglichkeit im Einzelfall erfolgen.[112]

Im Fall eines Widerspruchs des Verantwortlichen sehen in der Praxis viele Vertragsmuster eine Kündigungsmöglichkeit vor. Derartige Vereinbarungen sind nur zulässig, soweit dem Verantwortlichem tatsächlich noch eine Entscheidungsfreiheit bezüglich des Sub-Dienstleisters verbleibt. Dies wäre z.B. bei einer zu kurzen Kündigungsfrist fraglich, wenn dem Verantwortlichen eine Migration zu einem anderen Dienstleister in dieser Zeit unmöglich wäre.[113]

---

[109] Art 32 Abs 1 DSGVO

[110] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018): 159

[111] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018): 159

[112] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018): 140

[113] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018): 141

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3.3 Standards und Frameworks

Neben den verbindlichen Rechtvorschriften haben sich auch eine Vielzahl an Standards und Zertifizierungen etabliert. Diese Zertifizierungen ermöglichen es einem Cloud-Provider die Einhaltung gewisser Prozesse und Standards durch eine neutrale Stelle überprüfen und zertifizieren zu lassen.

Neben den generellen Prozess-Zertifizierungen wie ISO[114] haben sich zahlreiche Branchen auf spezielle Zertifizierungen geeinigt, welche Cloud-Provider erfüllen müssen, wenn diese Dienstleistungen anbieten wollen.[115]

Abbildung 4: Übersicht der Standards und Frameworks[116]

Es gibt eine Vielzahl an unterschiedlichen Standards und Zertifizierungen. Abbildung 4 gibt eine Übersicht über die am meist verbreiteten, Abbildung 5 stellt ihre Beziehung zueinander dar.

---

[114] ISO.org. „ISO.“ https://www.iso.org/home.html (zugegriffen: 20.10.2020)

[115] Becker, Jack, and Elana Bailey. "A comparison of IT governance & control frameworks in cloud computing." (2014)

[116] Cloud Industry Forum. „8 criteria to ensure you select the right cloud service provider“ https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider (zugegriffen: 20.10.2020): Certifications & Standards

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

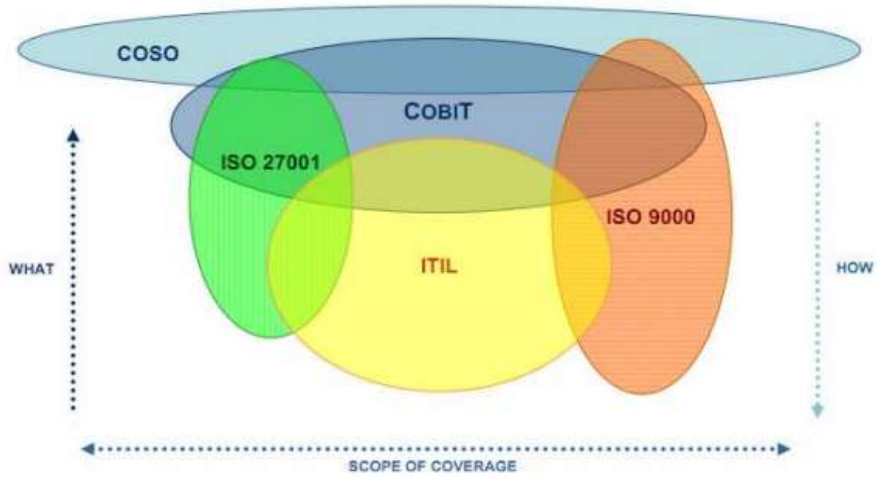

Abbildung 5: Beziehungen der unterschiedlichen Frameworks[117]

3.3.1 ISO Standards

Die „International Organisation for Standardisation“ (ISO) hat eine Vielzahl von Standards, die für Cloud-Provider interessant sind. Für den Datenschutz und das Recht auf Vergessen sind im Konkreten zwei von großer Bedeutung. Hierbei handelt es sich um ISO 27001[118] sowie ISO 27018[119]. Generell richten sich diese Standards vornehmlich an Geschäftskunden und nicht direkt an Privatanwender. Daraus ergibt sich, dass nicht alle Cloud-Provider diese Zertifizierungen anwenden. Primär sind sie für jenen Cloud-Provider relevant, die sich auf Enterprise-Kunden fokussieren. Cloud-Provider wie Amazon, Google oder Microsoft setzten auf diese Zertifizierungen, SaaS Anbieter wie Facebook geben hingegen öffentlich nicht bekannt, ob sie sich an diese Richtlinien halten.

---

[117] Becker, Jack, and Elana Bailey. "A comparison of IT governance & control frameworks in cloud computing." (2014)

[118] ISO. “ISO/IEC 27001 Information Security Management.” https://www.iso.org/isoiec-27001-information-security.html (zugegriffen: 20.10.2020)

[119] ISO. “ISO/IEC 27018:2019 Information Technology – Security techniques” https://www.iso.org/standard/76559.html (zugegriffen: 20.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Standard	Number of certificates in 2016	Number of certificates in 2015	Change	Change in %
ISO 9001**	1106356	1034180	72176	+7%
ISO 14001***	346189	319496	26693	+8%
ISO 50001	20216	11985	8231	+69%
ISO 27001	33290	27536	5754	+21%
ISO 22000	32139	32061	78	0
ISO/TS 16949	67358	62944	4414	+7%
ISO 13485	29585	26255	3330	+13%
ISO 22301	3853	3133	720	+23%
ISO 20000-1	4537	2778	1759	+63%
ISO 28000	356			
ISO 39001	478			
TOTAL	1,644,357	1,520,368		+8%

Abbildung 6: Übersicht der ISO Zertifizierungen[120]

In den letzten Jahren hat es einen stetigen Zuwachs an Institutionen gegeben, die sich den jeweiligen ISO Standards unterwerfen.

Die ISO 27001[121] spezifiziert ein Informationssicherheits-Managementsystem (ISMS) und beschreibt damit eine Anzahl von Aktivitäten für das Management von Informationsrisiken.

[120] ISO.org "The ISO Survey of Management System Standard Certifications" https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2 (zugegriffen: 1.2.2020)

[121] ISO.org „ISO/UEC 27001 Information Security Management." https://www.iso.org/isoiec-27001-information-security.html (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Abbildung 7: Übersicht ISO 27001 Standard[122]

Abbildung 7 gibt eine Übersicht der Komponenten, die in dem ISO 20701 Standard geregelt werden. Im Konkreten beschreibt der Standard 114 Kontrollen, die eine Organisation umsetzen muss, um ein Zertifikat zu erhalten. Diese Kontrollen beschäftigen sich mit unterschiedlichen Bereichen, wie z.B: Informationssicherheit, Inventar-Management, Zugangskontrollen, Kryptographie oder Zulieferer-Beziehung. Interessant ist, dass der Standard für eine Klassifizierung von Daten plädiert. Diese Klassifizierung wird auch für die notwendigen Aktionen beim Löschen der Daten herangezogen und gilt insbesondere für die Vernichtung von Datenträgern, auf denen klassifizierte Daten gespeichert wurden. ISO 27001 regelt hier im Konkreten zwei spezifischen Kontrollen:

[122] ISO. „ISO/IEC 27002:2013“ http://www.iso27001security.com/html/27002.html (zugegriffen: 1.2.2020): Contents of ISO/IEC 27002

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

"(-) Whenever a media shall be discarded, the use of procedures should be considered to ensure proper information disposal (control A.8.3.2 – Disposal of media).

….

(-) Equipment containing storage media shall be verified to ensure it is free of sensitive information prior to disposal or re-use (control A.11.2.7 – Secure disposal or reuse of equipment)." [123]

Die Kontrollen welche ISO 27002 vorsieht, können wie folgt beschrieben werden:

- Die Löschvorgänge sollen im Verhältnis zu der Klassifizierung der Daten stehen.

  Interessant hierbei ist, dass der Standard auf die Umsetzung einer Klassifizierung von Daten verweist, diese im Standard selbst aber nicht vorgibt. Sehr häufig verwenden Unternehmen eine 4-stufige Klassifizierung von Daten:[124]

  - Confidential (top confidentiality level)
  - Restricted (medium confidentiality level)
  - Internal use (lowest level of confidentiality)
  - Public (everyone can see the information)

  Dabei muss jene Person, die das Dokument erstell, die richtige Klassifizierung selbst durchführen. Neue Ansätze wie in O365 versuchen Anwender dabei zu unterstützen und setzen AI Methoden ein, um Vorschläge für die Klassifikation zu erstellen.[125]

[123] ISO. „ISO/IEC 27002:2013" http://www.iso27001security.com/html/27002.html (zugegriffen: 1.2.2020): Section 11

[124] Aggarwal, Charu C. "Data classification." *Data Mining*. Springer, Cham, 2015.

[125] Office 365. „Data Classification Overview." https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide (zugegriffen: 9.09.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Daten, die sicher gelöscht werden müssen, benötigen eine Identifikation. Dies kann mittels Wasserzeichen oder anderen Technologien sichergestellt werden.

- Das Mischen unterschiedlicher Speichermedien erhöht die Sicherheit und erschwert die Wiederherstellung gelöschter Daten.

- Das Löschen von sensiblen Daten sollte rückverfolgbar sein.

Wie Abbildung 8 zeigt, nahm die Verbreitung von ISO 27001 speziell in Europa und Asien verstärkt zu, wohingegen Unternehmen in Nordamerika noch immer einen sehr geringen Zertifizierungsstand aufweisen. Dies ist insofern ein Problem, da die meisten SaaS Angebote in Nordamerika zur Verfügung gestellt werden. Ausnahmen hierbei sind Amazon, Google oder Microsoft, die auch ihre nordamerikanischen Rechenzentren bereits nach ISO 27001 zertifiziert haben.

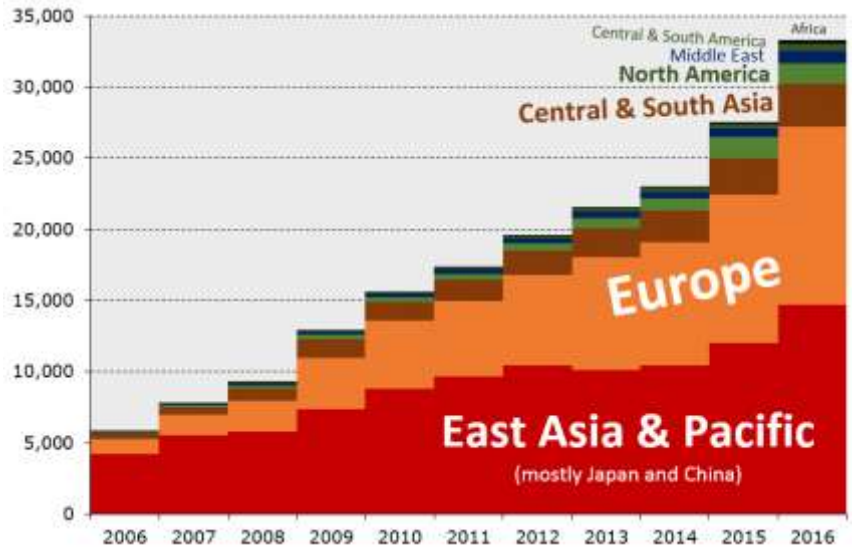

Abbildung 8: Verbreitung von ISO 27001[126]

[126] ISO. „ISO/IEC 27001:2013“ https://www.iso27001security.com/html/27001.html (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3.3.1.1 ISO 27017

Im Gegensatz zu ISO 27001/27002 behandelt der Standard ISO 27017 Sicherheitsrechtlinien für Cloud-Provider und Cloud Kunden[127]. Da es sich hierbei nicht um einen Management Standard handelt, können Organisationen sich nicht nach ISO 20017 standardisieren lassen.

Um dies zu erreichen, erweitert ISO 27017 die existierenden ISO 27001/27002 um sechs neue Kontrollen.

- *6.3.1 Shared roles and responsibilities within a cloud computing environment*
- *8.1.5 Removal of cloud service customer assets*
- *9.5.1 Segregation in virtual computing environments*
- *9.5.2 Virtual machine hardening*
- *12.1.5 Administrator's operational security*
- *12.4.5 Monitoring of cloud services*
- *13.1.4 Alignment of security management for virtual and physical networks*[128]

Im speziellen die Regeln für das Löschen von Cloud-Service Daten definieren wie Cloud-Provider mit Daten umgehen müssen, sofern der Kunde die Nutzung der Cloud-Services nicht mehr in Anspruch nehmen möchte.

3.3.1.2 ISO 27018

Wie ISO 27017 ist auch ISO 27018 an Cloud-Provider und Kunden gerichtet. Primär regelt der Standard den Umgang mit „Personally Identifiable

[127] ISO. „ISO/IEC 27017:2015" https://www.iso27001security.com/html/27017.html (zugegriffen: 1.2.2020)
[128] ISO. „ISO/IEC 27017:2015" https://www.iso27001security.com/html/27017.html (zugegriffen: 5.5.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Information“ (PII)[129] und welche Sicherheitsmechanismen Cloud-Provider sowie Cloud Kunden anwenden sollten, um die Sicherheit der Informationen zu gewährleisten.[130]

Im Großen und Ganzen geht es bei ISO 27018 um folgende Themen:

- Kunden sollen wissen, wo ihre Daten gespeichert werden;
- Kundendaten werden ohne ausdrückliche Zustimmung nicht für Marketingaktivitäten verwendet;
- Kunden sollen darüber Bescheid wissen, was mit ihren PII Informationen passiert.

Im Konkreten verlangt ISO 27018, dass Cloud-Anbieter Regeln für das zurückgeben, Transferieren und sichere Löschen von personenbezogenen Daten (PII) dokumentiert haben und die Anforderungen von Kunden in Bezug auf diese Regeln in einer nachvollziehbaren Zeit durchführen können.

3.3.2 AICPA – SOC 1-3

Das „American Insitute of Certified Public Accountants“ wurde 1887 gegründet und ist ein nationaler Zusammenschluss von mehr als vierhunderttausend Wirtschaftsprüfern in den USA. Ursprünglich gegründet, um Standards für die wirtschaftliche Prüfung von Unternehmen zu definieren, hat es sich im Laufe der Zeit auch mit anderen, für Unternehmen wichtigen, Aspekten beschäftigt. [131]

Zu einem der wichtigsten Audit Standards hat sich der Katalog der „System and Organisation Controls“ (SOC) entwickelt. Im Gegensatz zu SOC-1, welches sich ausschließlich um Sicherstellung der Einhaltung interner Kontrollen für die

[129] Balachander Krishnamurthy and Craig E. Wills. "On the leakage of personally identifiable information via online social networks.", Association for Computing Machinery, (2009): 7
[130] ISO. “ISO/IEC 27018:2019” https://www.iso27001security.com/html/27018.html (zugegriffen: 1.2.2020)
[131] AICPA. „American Institute of Certified Public Accountants.“ https://www.aicpa.org/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Finanzberichterstattung kümmert, adressieren SOC-2 und SOC-3 vordefinierte Standard-Benchmarks für Kontrollen in Bezug auf die Sicherheit, Verfügbarkeit, Verarbeitungsintegrität und Vertraulichkeit eines Systems und seiner Informationen. [132]

	Anwender	Was	Warum
SOC-1	Management der Service-Organisation, Kunden und deren Auditoren	Steuerelemente, die für die Finanzberichterstattung von Benutzern relevant sind	Prüfung der Finanzen
SOC-2	Management der Service-Organisation, Kunden und deren Auditoren, Aufsichtsbehörden	Regeln hinsichtlich einer Systemsicherheit, Verfügbarkeitsintegrität, Vertraulichkeit oder Datenschutz	Steuerung von Risiko und Compliance Programmen sowie Beaufsichtigung und sorgfältige Prüfung der Regel
SOC-3	Jeder Anwender, der sicherstellen will, dass die Regeln eingehalten werden	Bestätigung und Prüfbericht über die Umsetzung der Regeln und Kontrollen	Zur öffentlichen Bestätigung der Einhaltung

Tabelle 7 SOC Übersicht

3.3.3 Cloud Security Alliance (CSA)

Die Cloud Security Alliance ist eine non-profit Organisation, die 2008 gegründet wurde und es sich zum Ziel gemacht hat, Best Practices zu definieren, um ein

[132] AICPA. "System and Organization Controls: SOC Suite of Services." https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html (zugegriffen. 1.5.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

sicheres Cloud Computing zu gewährleisten. Um diese umzusetzen, gibt es unterschiedliche Abteilungen und Zugänge die sowohl Cloud-Service-Provider als auch Kunden unterstützen. Zu den wichtigsten zählen der Security Guide sowie die Security Trust and Assurance Registry, die in den nächsten Kapiteln näher erklärt werden.[133]

3.3.3.1 Security Guide

Um Kunden eine einfachere und bessere Möglichkeit zu bieten, die Security und Compliance in der öffentlichen Cloud zu adressieren, hat die CSA in einer ihrer Arbeitsgruppen einen Leitfaden ausgearbeitet.

Der Leitfaden wendet sich primär an Führungskräfte und Anwender, die Cloud-Services benutzen möchten. Für diese beschreibt der Leitfaden in 13 unterschiedlichen Domänen Best Practices. Für alle Domänen gibt der Leitfaden eine Liste an Empfehlungen und Anforderungen, welche gemessen und auditiert werden können.

Zusätzlich zu den 13 Domänen gibt der Leitfaden auch ein einfaches Framework an, um die Cloud-Risiken zu bewerten und abzuschätzen. Dieses Framework kann als Basis verwendet werden, um zu entscheiden, ob spezielle Daten und Applikationen in die Cloud verschoben werden sollen. [134]

Das Framework erlaubt hierbei:

- Identifikation von möglichen Cloud-Deployment-Werten
- Eine Abbildung der Werte zu potenziellen Betriebsmodellen
- Evaluierung möglicher Cloud-Service-Provider und Modelle
- Herausbildung notwendiger Datenflüsse

---

[133] CSA. „Cloud Security Alliance.“ https://cloudsecurityalliance.org (zugegriffen: 1.2.2020)
[134] CSA. „CSA-Guidance.“ https://github.com/cloudsecurityalliance/CSA-Guidance (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3.3.3.2 CSA Security, Trust and Assurance Registry (STAR)

Um eine generelle Basis für die Bewertung der Sicherheit von Cloud-Providern zu gewährleisten hat die CSA ein eigenes Zertifikations-Programm (CSA STAR)[135] entwickelt, welches sich weltweit zu dem am weitest verbreiteten und angenommen Programmen dieser Art entwickelt hat. Im Wesentlichen besteht STAR aus drei aufeinander aufbauenden Bereichen:[136]

- LEVEL ONE: Selbst Evaluierung
- LEVEL TWO: Zertifizierung
- LEVEL THREE: Auditierung

Abbildung 9: Übersicht Open Certification Framework[137]

[135] CSA. „CSA Security Trust Assurance and Risk (STAR).“ https://cloudsecurityalliance.org/star/ (zugegriffen: 1.2.2020)

[136] Samani, Raj, Honan, Brian, Reavis, Jim, Jirasek, Vladimir, Katsaropoulos, Chris, Rearick, Benjamin, Govindaradjane, Punithavathy, and Rogers, Mark. „CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security.“ Waltham, Maryland: Elsevier : Syngress, (2015): Chapter 8

[137] CSA. „Open Certification Framework“ https://cloudsecurityalliance.org/star/levels/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Diese drei Bereiche basieren wiederum auf drei Sicherheitsebenen:

- CSA Cloud Controls Matrix (CCM)[138]

  Hierbei handelt es sich um ein Framework, das Organisationen mit einem strukturierten Vorgehensmodell auf dem Weg in die Cloud unterstützt. Die Matrix unterscheidet zwischen 16 Domänen (z.B. Applikation & Interface Security, Data Security & Information Life Cycle Management, …). Diese werden auf Basis der Architektur und bezugnehmend auf das Betriebsmodell (SaaS, PaaS, IaaS) und hinsichtlich der Verantwortung (Service-Provider oder Kunde) bewertet. Zusätzlich verweist die Matrix auf unterschiedliche Zertifizierungen (z.B.: COBIT, CSA, ENISA, EUDPD, FedRamp, HIPAA, ISO/IEC, ITAR, PCI, …) und beschreibt, wo diese die jeweiligen Bereiche adressieren.[139]

- Consesusus Assemsent Inaitaitive Questionare (CAIQ)

  Basierend auf dem CCM bietet der CAIQ eine Anzahl an Fragen, die ein Auditor an Kunden sowie Cloud-Provider richten kann um, die Einhaltung der Cloud Control Matrix sowie der CSA Best Practices sicherzustellen.[140]

- CSA Code of Conduct for GDPR Compliance (CSA CoC for GDPR) [141]

  Die Einhaltung von Datenschutzbestimmungen wird zunehmend risikobasiert. Um Cloud-Service-Provider und auch deren Kunden eine Lösung zur Einhaltung der GDPR Richtlinien zur Verfügung zu stellen, hat die CSA in diesem Dokument transparente Regeln ausgearbeitet mit dem Ziel:

---

[138] CSA. „Cloud Controls Matrix (CCM)“ https://cloudsecurityalliance.org/research/cloud-controls-matrix/ (zugegriffen: 1.2.2020)

[139] Samani, Raj, Honan, Brian, Reavis, Jim, Jirasek, Vladimir, Katsaropoulos, Chris, Rearick, Benjamin, Govindaradjane, Punithavathy, and Rogers, Mark. „CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security.“ Waltham, Maryland: Elsevier : Syngress, (2015): Chapter 6

[140] CSA. „Working Group Consensus Assessments.“ https://cloudsecurityalliance.org/group/consensus-assessments/ (zugegriffen: 1.2.2020)

[141] Erwägungsgrund 83 und Artikel 25, 32, 33, 34 und 35 DSGVO

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Cloud Kunden ein Tool zur Verfügung zu stellen, welches es ermöglicht die Umsetzung des Schutzes von persönlichen Daten der unterschiedlichen Cloud-Provider zu evaluieren.
- Cloud Solution Providern unabhängig von ihrer Größe oder geografischen Lage Unterstützung zu geben, um mit den neuen Anforderungen der GDPR umzugehen und Kunden eine strukturierte und einheitliche Möglichkeit zu geben, die Umsetzung der unterschiedlichen CSPs zu vergleichen.

3.3.4 Übersicht weltweit relevanter Standards und Zertifizierungen

Weltweit gibt es eine große Anzahl an unterschiedlichen Standards und Zertifizierungen. Die hier angeführte Liste bietet eine gute Übersicht, stellt aber keinen Anspruch auf Vollständigkeit.

Name	Beschreibung	Reference
AICPA 2009 TSC Map	Eine Abbildung der "Trust Service Criteria" auf unterschiedliche Frameworks (z.B. ISO 27001. COBIT5)	https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/mappingsrelevanttothesocsuiteofservices.html
AICPA Trust Service Criteria (SOC 2 SM Report)	Bericht über Kontrollen in einer Serviceorganisation, die für Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit oder Datenschutz relevant sind	https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/trustdataintegritytaskforce.html
AICPA 2014 TSC	Die TSC sind Kontrollkriterien für die Verwendung bei Beglaubigungs- oder	https://www.aicpa.org/interestareas/frc/assuranceadvisoryser

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

	Beratungsaufträgen zur Bewertung und Meldung von Kontrollen über Informationen und Systeme.	vices/trustdataintegritytaskforce.html
BITS Shared Assessments AUP	Das BITS Shared Assessments-Programm ermöglicht es Finanzinstituten, die Sicherheitskontrollen wichtiger IT-Dienstleister zu bewerten und die Einhaltung gesetzlicher Vorschriften zu gewährleisten.	https://sharedassessments.org/
BSI Germany	Der Anforderungskatalog C5 kann durch ein Audit analog zu ISAE 3000 beim Cloud-Anbieter geprüft werden, woraus ein so genannter SOC 2-Bericht über die Angemessenheit und Wirksamkeit der Kontrollen entsteht.	https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudZertifizierung/CloudZertifizierung_node.html
Canada PIPEDA	Ist ein kanadisches Gesetz, das regelt, wie private Sektoren persönliche Informationen in kommerziellen Aktivitäten sammeln, verwenden und offenlegen.	https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/
CCM	Die Cloud Controls Matrix (CCM) der Cloud Security Alliance wurde speziell entwickelt, um grundlegende Sicherheitsgrundsätze für Cloud-Anbieter bereitzustellen und potenzielle Cloud-Kunden bei der Bewertung des allgemeinen Sicherheitsrisikos	https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

	eines Cloud-Anbieters zu unterstützen.	
CIS-Foundation	CIS entwickelte einen Benchmark für Konfigurationsrichtlinien für verschiedene Technologiegruppen, um Systeme gegen die sich heute entwickelnden Cyber-Bedrohungen zu schützen.	https://www.cisecurity.org/cis-benchmarks/
COBIT 4.1/5	Control Objectivies for Information and Related Technologies COBIT ist ein IT-Governance-Framework und ein unterstützendes Toolset, dass es Managern ermöglicht, die Lücke zwischen Kontrollanforderungen, technischen Problemen und Geschäftsrisiken zu schließen.	http://www.isaca.org/cobit/pages/default.aspx
COPPA	Websites, auf denen Informationen von Kindern unter dreizehn Jahren gesammelt werden, müssen das Online-Datenschutzgesetz (COPPA) der Federal Trade Commission (FTC) einhalten.	http://www.coppa.org/coppa.ht
CSA Enterprise Architecture (formerly Trusted Cloud Initiative)	Die Enterprise Architecture ist sowohl eine Methodik als auch eine Reihe von Tools, mit denen Sicherheitsarchitekten, Unternehmensarchitekten und Risikomanagementexperten eine Reihe von Lösungen nutzen	https://cloudsecurityalliance.org/group/enterprise-architecture/#_overview

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

	können, die ihre gemeinsamen Anforderungen erfüllen, um einschätzen zu können, wo sich ihre interne IT und ihre Cloud-Anbieter befinden	
CSA Guidance	CSA Security Guidance für kritische Bereiche des Cloud Computing zielt darauf ab, eine stabile und sichere Basis für Cloud-Operationen zu schaffen. Diese Bemühungen bieten eine praktische, umsetzbare Roadmap für Manager, die das Cloud-Paradigma sicher übernehmen möchten.	https://cloudsecurityalliance.org/group/security-guidance/#_overview
ENISA	Die ENISA, die von einer Expertengruppe aus Vertretern von Industrie, Wissenschaft und Regierungsorganisationen unterstützt wird, hat im Rahmen des Projekts "Emerging und Future Risk Framework" eine Risikobewertung des Geschäftsmodells und der Technologien des Cloud Computing durchgeführt.	https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
GDPR/ DSGVO	Vorgänger Version von der eine 1995 verabschiedete EU-Richtlinie, die die Verarbeitung personenbezogener Daten in der Europäischen Union regelt. Es ist ein wichtiger Bestandteil des EU-Datenschutzrechts und der Menschenrechte.	https://ec.europa.eu/info/law/law-topic/data-protection_en

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

FedRAMP Security Controls	FedRAMP definiert eine Reihe von Steuerelementen für Systeme mit niedriger und mittlerer Sicherheitsauswirkung basierend auf NIST-Basissteuerelementen (NIST SP 800-53, überarbeitet) mit einer Reihe von Steuererweiterungen, die die einzigartigen Sicherheitsanforderungen von Cloud Computing betreffen.	https://www.fedramp.gov
FERPA	Das Familiengesetz über Bildungsrechte und Datenschutz aus dem Jahr 1974 (FERPA) ist ein US-Bundesgesetz, das die Privatsphäre von Schüleraufzeichnungen schützt. Das Gesetz gilt für alle Schulen, die Mittel im Rahmen eines anwendbaren Programms des US-Bildungsministeriums erhalten	https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
GAPP	(GAPP) ist ein Rahmenwerk, das Chartered Accountants und Certified Public Accountants bei der Erstellung eines wirksamen Datenschutzprogramms zur Verwaltung und Prävention von Datenschutzrisiken unterstützen soll.	
HIPAA / HITECH Act	HIPAA ist die Gesetzgebung der Vereinigten Staaten, die	https://www.hhs.gov/hipaa/index.html

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

	Datenschutz- und Sicherheitsbestimmungen für den Schutz medizinischer Informationen enthält.	
HITRUST CSF	HITRUST CSF bietet Unternehmen die notwendige Struktur in Bezug auf Informationssicherheit, die auf die Gesundheitsbranche zugeschnitten ist.	https://hitrustalliance.net/hitrust-csf/
ISO/IEC 27001:2013	legt die Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems im Kontext der Organisation fest.	https://www.iso.org/standard/54534.html
ISO/IEC 27002:2013	Gibt Richtlinien für organisatorische Informationssicherheitsstandards und Informationssicherheitsmanagementpraktiken einschließlich der Auswahl, Implementierung und Verwaltung von Kontrollen unter Berücksichtigung der Informationssicherheitsrisikoumgebung(en) der Organisation	https://www.iso.org/standard/54533.html
ISO/IEC 27017:2015	Gibt Richtlinien für Informationssicherheitskontrollen vor, die für die Bereitstellung und Nutzung von Cloud-Diensten gelten.	https://www.iso.org/standard/43757.html

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

ISO/IEC 270018:2015	Legt allgemein akzeptierte Kontrollziele, Kontrollen und Richtlinien für die Implementierung von Maßnahmen zum Schutz personenbezogener Daten (PII) gemäß den Datenschutzgrundsätzen in ISO / IEC 29100 für die öffentliche Cloud-Computing-Umgebung fest.	https://www.iso.org/standard/61498.html
NIST SP800-53	Eine Datenbank, die Sicherheitskontrollen und die damit verbundenen Bewertungsverfahren definiert.	https://nvd.nist.gov/800-53
NZISM	Ist das Handbuch der neuseeländischen Regierung zur Informationssicherheit und Sicherheit von Informationssystemen.	https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/
PCI DSS	Rahmen von Spezifikationen, Werkzeugen, Messungen und Unterstützungsressourcen, um Organisationen zu helfen, den sicheren Umgang mit Karteninhaberinformationen bei jedem Schritt sicherzustellen	https://www.pcisecuritystandards.org/document_library

Tabelle 8 Übersicht weltweiter Standards und Zertifizierungen

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 4
Löschung von Daten in der Cloud

4.1 Rechtliche Aspekte

4.1.1 Das Recht auf Vergessenwerden

4.1.1.1 Problemstellung und Definition

Das Cloud Computing bietet zahlreiche rechtliche Herausforderungen im Bereich des Datenschutzes, wobei speziell das Löschen von Daten eine der größten ist, weil dieses Thema nicht umfassend rechtlich geregelt und die technische Implementierung problematisch ist. Dank der Cloud-Services kann man enorme Datenmengen sehr günstig speichern, was viele Menschen dazu verleitet Daten generell nicht zu löschen. Einigen Personen gehen mit ihren persönlichen Daten sorglos um, veröffentlichen Fotos in sozialen Netzwerken, ohne daran zu denken, ob und wie diese Daten später gelöscht werden können. Was einmal in der Cloud bzw. im Internet veröffentlicht wurde, kann sehr einfach kopiert werden, diese Kopien endgültig zu löschen, ist in den meisten Fällen kaum möglich.

Für das Löschen von Daten wurden zahlreiche Konzepte entwickelt. Als "Recht auf Vergessenwerden" umschreibt Viktor Mayer-Schönberger, dass elektronisch gespeicherte Informationen mit einem Ablauf- bzw. Verfallsdatum auszustatten sind und die Information nach Ablauf dieses Datums durch ein Programm oder Betriebssystem automatisch gelöscht werden soll.[142] Nach diesem Vorschlag soll die digitale Welt genauso vergessen, wie die Menschen. Er schlägt kein DRM-System[143] vor, sondern will den Nutzer ständig damit konfrontieren, wie lange sie

[142]Nolte, Norbert. “Zum Recht Auf Vergessen Im Internet: Von Digitalen Radiergummis Und Anderen Instrumenten.” Zeitschrift Für Rechtspolitik, vol. 44, no. 8, (2011): 236

[143] Stephan Kolter. „Digital Rights Management: Eine Lösung für die digitale Krise des Urheberrechts?“ VDM Verlag Dr. Müller (2008): 45ff

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

die Information aufbewahren möchte. Seiner Meinung nach wäre die Implementierung sehr einfach. Die Softwarehersteller sollte man dazu verpflichten, ein Verfallsdatum zu den Metadaten hinzufügen.[144]

Technisch gesehen gibt es unterschiedliche Möglichkeiten das Löschen von Daten umzusetzen. Da das Internet sehr offen gestaltet ist, muss das Prinzip eines „digitalen Radiergummis" in jeden Fall Plattform-, Format- und Betreiberunabhängig aufgebaut werden. X-pire! (siehe Kapitel 4.2.2.1) hat hier bereits ein System auf Basis von Verschlüsselungstechnologien für Fotos entwickelt, welches theoretisch auch auf andere Inhalte erweiterbar wäre. Die Erweiterung von X-pire!, das sogenannte Data Revocation Service (DRS) (siehe Kapitel 4.2.2.5), beschreibt einen Ablauf, wie Daten zwischen Besitzern und Nutzern sicher ausgetauscht und deren Verwendung nach einer gewissen Zeit wieder unterbunden werden kann.

4.1.1.2 Datenschutzrichtlinie (95/46/EG)

Am 25.5.2018 ist die Datenschutz-Grundverordnung (im Folgenden: DSGVO) in Kraft getreten. Das Löschen von Daten wurde davor auf Europarechtsebene in der Richtlinie 95/46/EG des Europäischen Parlaments und Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten und zum freien Datenverkehr (im Folgenden: EU-Datenschutzrichtlinie) geregelt. Die EU-Datenschutzrichtlinie umfasst Prinzipen, die auf Europarechtsebene bereits das „Recht auf Vergessenwerden" untermauert:

> *„Auskunftsrecht*
>
> *Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen folgendes zu erhalten: […]*

[144] Viktor Mayer-Schönberger. „Interview: Daten brauchen ein Verfallsdatum" http://www.golem.de/0804/58721.html (zugegriffen:15.8.2019)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;

c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b) durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.“[145]

Die Bestimmungen der EU-Datenschutzrichtlinie umfassten eine Pflicht zur Berichtigung oder zum Löschen von Daten, wenn die Verarbeitung nicht im Sinne der Richtlinie erfolgt ist. Sie beinhaltet auch eine Mitteilungspflicht gegenüber Dritten, an denen die Daten übermittelt wurden, sofern es nicht unmöglich oder nicht mit unverhältnismäßigem Aufwand verbunden ist.

4.1.1.3 Datenschutz-Grundverordnung (DSGVO)

Da die Regelungen der EU-Datenschutzrichtlinie nicht zweitgemäß waren, mussten die Bestimmungen des Datenschutzrechtes für die moderne digitale Welt aktualisiert werden. Bei der DSGVO handelt es sich um eine Verordnung der Europäischen Union, die die EU-Datenschutzrichtlinie abgelöst hat. Mit ihr werden Regeln für die Verarbeitung von personenbezogenen Daten festgelegt.

Die DSGVO ist in den Mitgliedstaaten der EU unmittelbar anwendbar und bedarf keine zusätzliche Umsetzung. Sie soll auch für Unternehmen gelten, die ihren Sitz außerhalb der Europäischen Union haben, sich mit ihren Angeboten aber an EU-Bürger wenden (z.B. Facebook und Google).[146] Die DSGVO ist viel mehr als die Verankerung des „Rechtes auf Vergessenwerden“, es handelt sich um eine globale Reform des Datenschutzrechtes auf Europarechtsebene. Im Hinblick auf den Schwerpunkt dieser Diplomarbeit wird in diesem Zusammenhang allerdings nur das „Recht auf Vergessenwerden“ untersucht.

---

[145] Artikel 12 EU-Datenschutzrichtlinie

[146] Jürgen Kühling, Manuel Klar, Florian Sackmann, "Datenschutzrecht." 4. Auflage. Heidelberg 2018, ISBN 978-3-8114-4571-0: 100

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die DSGVO enthält das Recht auf Vergessenwerden und auf Löschung, welches von den für die Verarbeitung der Daten Verantwortlichen umzusetzen ist:

Recht auf Löschung („Recht auf Vergessenwerden“)

“(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen."[147]

Im Art 17 Abs 1 DSGVO wird ein Löschungsanspruch geregelt, wenn die Daten zu der Erreichung des Zwecks nicht mehr notwendig sind, die betroffene Person ihre Einwilligung widerruft oder deren Befristung abläuft, Widerspruch eingelegt

[147] Art. 17 DSGVO

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

wird oder die Verarbeitung aus anderen Gründen nicht mit der DSGVO vereinbar ist. Es wird auch geregelt, wann eine Löschung ausnahmsweise nicht vorzunehmen ist, und wann die Daten zu sperren sind. Darüber hinaus werden auch Regelungen hinsichtlich der Folgen der Sperrung, der Pflicht des Verantwortlichen Datenbeständen regelmäßig in Bezug auf die Löschungspflichten zu überprüfen und der Umgehungsverbote getroffen.

In der DSGVO folgt eine Löschungspflicht unverändert aus dem Erforderlichkeitsprinzip, das nunmehr um das Prinzip der Datenvermeidung und Datensparsamkeit in Art 5 DSGVO ergänzt wurde.[148]

Eine Löschungspflicht nach dem DSGVO hängt nicht vom Verlangen des Betroffenen ab. Nur bei einem Widerspruch (Art 19 DSGVO) kommt es auf dessen Tätigwerden an. Nach Art 14 Abs 1 und Art 15 Abs 1 DSGVO sind die Verantwortlichen verpflichtet Speicherfristen mitzuteilen.

Nach *Hornburg/Hoffmann* sieht man in der Einführung von Verfallsdaten, nach deren Überschreitung die betreffenden Daten zu löschen sind, nicht die Verankerung des Rechtes auf Vergessenwerden:

> *„Art.17 Abs.1 DSGVO enthält zwar die Löschpflicht nach Fristablauf, wenn eine Einwilligung für eine bestimmte Speicherfrist gegeben wurde, dies war aber auch nach bisherigem Recht möglich und ist deshalb nur eine Klarstellung. Die Verarbeitungsbefugnisse sind auch in der DSGVO nicht befristet, sondern stehen unter der Bedingung, dass nicht einer der von Art.17 Abs.1 DSGVO konkretisierten Löschgründe vorliegt. Wenn die Verantwortlichen also Speicherdauern angegeben müssen, dann handelt es sich hier um Prognosen, die – wenn der Zweck unverändert fortbesteht oder sich für die Weiterverarbeitung ein anderer zulässiger Grund ergibt – keine Auswirkungen haben.“*[149]

---

[148] Gerrit Hornung/ Kai Hoffmann. „Ein »Recht auf Vergessenwerden«? Anspruch und Wirklichkeit eines neuen Datenschutzrechts“, JZ 68 (2013): 166

[149] Gerrit Hornung/ Kai Hoffmann. „Ein »Recht auf Vergessenwerden«? Anspruch und Wirklichkeit eines neuen Datenschutzrechts“, JZ 68 (2013): 166

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Eine wesentliche Bestimmung ist Art 17 Abs 2 DSGVO, sie regelt, wie mit öffentlich gemachten Daten zu verfahren ist. Nach dieser Bestimmung ist der Verantwortliche verpflichtet, weitere Verantwortliche, die die zu löschenden Daten verarbeiten, über ein Verlangen des Betroffenen zur Löschung von Daten zu informieren. Im Hinblick darauf, dass in der DSGVO nicht genau formuliert ist, welche Technologie und Implementierungskosten angemessen sind, könnten Datenverarbeiter einen Löschungsantrag öffentlich gemachter Daten ablehnen und mit dem unverhältnismäßigen Aufwand begründen.

In der DSGVO ist nicht konkret dargestellt, welcher Aufwand verhältnismäßig ist. In den Erwägungsgründen ist nur erwähnt, dass in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, der Verantwortliche eine Datenschutz-Folgenabschätzung durchführen soll, in der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden. Art 35 DSGVO regelt die Datenschutz-Folgenabschätzung und wann diese erforderlich ist.[150]

> *„Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:*
>
> *(a) eine systematische und umfassende Bewertung persönlicher Aspekte von natürlichen Personen handelt, die auf automatisierte Verarbeitung einschließlich Profiling gründet, welche ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen*
>
> *(b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10*

[150] Erwägungsgrund (84) DSGVO

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

(c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche „[151]

4.1.1.4 Urteil des EuGHs zu C 131/12

In diesem Urteil hat der EuGH entschieden, dass der Betreiber einer Internetsuchmaschine für die Verarbeitung von personenbezogenen Daten verantwortlich ist, welche Dritte auf Webseiten veröffentlichen.

Dieser Entscheidung zu Folge, kann sich jemand unter bestimmten Voraussetzungen, direkt an den Suchmaschinenbetreiber wenden, um eine Löschung zu erwirken.

Mario Costeja González, ein spanischer Staatsbürger, erhob bei der spanischen Datenschutzagentur (AEPD) eine Beschwerde gegen La Vanguardia Ediciones SL, die Herausgeberin einer in Spanien weitverbreiteten Tageszeitung, sowie gegen Google Spain und Google Inc. Gonzáles machte geltend, dass bei Eingabe seines Namens in der Google-Suchmaschine zwei Seiten der genannten Tageszeitung von 1998 angezeigt werden, auf welche die Versteigerung eines Grundstücks ersichtlich ist, welche im Zusammenhang mit einer Pfändung wegen Schulden stand. González beantragte, die Tageszeitung entweder zur Löschung oder zur Änderung der betreffenden Seiten zu verpflichten, damit die ihn betreffenden personenbezogen Daten dort nicht mehr angezeigt würden. Weiters beantragte er, Google anzuweisen, ihn betreffende personenbezogene Daten zu löschen oder zu verbergen, so dass diese weder in den Suchergebnissen noch in den Links zu der Tageszeitung erschienen, da die Pfändung seit Jahren vollständig erledigt sei und daher keine Relevanz mehr hatte.[152]

Die Beschwerde wurde von der spanischen Datenschutzagentur, soweit sie sich gegen die Tageszeitung richtete, zurückgewiesen, weil die Informationen

---

[151] Art 35 Abs 1 DSGVO

[152] Gerichtshof der Europäischen Union. „Pressemitteilung Nr. 70/14 - Urteil in der Rechtssache C-131/12“ http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

rechtmäßig veröffentlicht wurden. In Bezug auf Google wurde der Beschwerde stattgegeben. Google wurde daher aufgefordert, die betreffenden Daten aus dem Index zu entfernen. Google hat zwei Klagen auf Aufhebung der Entscheidung der spanischen Datenschutzagentur erhoben.[153]

Das zuständige spanische Gericht hat dem EuGH folgende Fragen zur Vorabentscheidung vorgelegt:[154]

a. Ist die Datenschutzrichtlinie auf Suchmaschinenbetreiber anzuwenden?
b. Ist die Datenschutzrichtlinie in Bezug auf Google Spain anwendbar, wenn der Server in der USA ist?
c. Hat jemand das Recht vom Suchmaschinenbetreiber die Entfernung von personenbezogenen Daten zu verlangen?

Der EuGH hat darauf wie folgt geantwortet:

a. Der Betreiber einer Suchmaschine, ist jener der automatisch, kontinuierlich und systematisch im Internet veröffentlichte Informationen aufspürt, eine „Erhebung" von Daten im Sinne der Richtlinie vornimmt. Das Auslesen, Speichen und Organisieren von Daten auf einem Server durch ein Indexprogramm und das Aufbewahren von Daten, um Ergebnisse an Nutzer weiterzugeben sind als Verarbeitungen im Sinne der Datenschutzrichtlinie anzusehen. Diese Vorgänge sind auch dann als Verarbeitung anzusehen, wenn sie ausschließlich Informationen enthalten, die bereits in den Medien veröffentlicht worden sind. Der Gerichtshof stuft den Suchmaschinenbetreiber, da dieser über die Zwecke und Mittel einer solchen Verarbeitung entscheidet, als den im Sinne der Richtlinie für die

[153] Gerichtshof der Europäischen Union. „Pressemitteilung Nr. 70/14 - Urteil in der Rechtssache C-131/12" http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

[154] Gerichtshof der Europäischen Union. „Fragen an den EUGH Rechtssache C-131/12" https://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=uriserv%3AOJ.C_.2012.165.01.0011.01.DEU (zugegriffen: 12.06.2018)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Verarbeitung „Verantwortlichen“ ein, der dafür zu sorgen hat, dass seine Tätigkeit den Anforderungen der Richtlinie entspricht.[155]

b. Bei Google Spain handelt es sich um eine Tochtergesellschaft von Google Inc. in Spanien und somit eine „Niederlassung“ im Sinne der Richtlinie. Bei der Verarbeitung personenbezogener Daten zum Betrieb einer Suchmaschine durch ein Unternehmen mit Sitz in einem Drittstaat, das aber in einem Mitgliedstaat eine Niederlassung besitzt, wird die Verarbeitung im Sinne der Richtlinie dieser Niederlassung ausgeführt.[156]

c. Privatpersonen haben unter bestimmten Voraussetzungen das Recht die Löschung von Links auf personenbezogene Informationen zu verlangen. Dabei ist zu berücksichtigen, dass das Internet eine sehr bedeutende Rolle in der modernen Gesellschaft hat - die Internetnutzer können von der gesuchten Person ein detailliertes Profil erstellen. Es ist ein angemessener Ausgleich zwischen dem Interesse an öffentlichen Informationen und den Grundrechten der betroffenen Person, insbesondere in Bezug auf das „Recht auf Achtung des Privatlebens“ und „Rechts auf Schutz personenbezogener Daten“, zu schaffen.[157] Auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten kann im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind. Das ist insbesondere der Fall, wenn sie diesen Zwecken in Anbetracht der verstrichenen Zeit nicht entsprechen, dafür

---

[155] Gerichtshof der Europäischen Union. „Urteil in der Rechtssache C-131/12“ http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

[156] Gerichtshof der Europäischen Union. „Urteil in der Rechtssache C-131/12“ http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

[157] Gerichtshof der Europäischen Union. „Urteil in der Rechtssache C-131/12“ http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

nicht oder nicht mehr erheblich sind oder darüber hinausgehen.[158] Mit dieser Entscheidung hat der EuGH die Grundlage für das Rechtes auf Vergessenwerden geschaffen. Nach dem EuGH handelt es sich dabei um kein absolutes Recht. Bei der Beurteilung, ob die Daten zu löschen sind, ist die Art und Sensibilität der Information, das Interesse der Öffentlichkeit Zugang zu den Informationen zu haben, sowie die Rolle der betreffenden Person im öffentlichen Leben zu berücksichtigen.[159]

4.1.1.5 Das Recht auf Löschung im österreichischen Datenschutzgesetz

§ 45 DSG regelt das Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung:

„(1) Jede betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung von unrichtiger sowie die Vervollständigung unvollständiger, sie betreffenden, personenbezogener Daten zu verlangen. Die Berichtigung oder Vervollständigung kann erforderlichenfalls mittels einer ergänzenden Erklärung erfolgen, soweit eine nachträgliche Änderung mit dem Dokumentationszweck unvereinbar ist. Der Beweis der Richtigkeit der Daten obliegt dem Verantwortlichen, soweit die personenbezogenen Daten nicht ausschließlich aufgrund von Angaben der betroffenen Person ermittelt wurden.

(2) Der Verantwortliche hat personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzüglich zu löschen, wenn

1. die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,

2. die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder

---

[158] InfoCuria. „Urteil des Gerichtshofes in Rechtssache C-131/12“ http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=DE (zugegriffen: 02.04.2018): Anmerkung Nr. 93

[159] InfoCuria. „Urteil des Gerichtshofes in Rechtssache C-131/12“ http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=DE (zugegriffen: 02.04.2018): Anmerkung Nr. 99

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

3. die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder

2. die personenbezogenen Daten für Beweiszwecke im Rahmen der Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe weiter aufbewahrt werden müssen.

Im Falle einer Einschränkung gemäß Z 1 hat der Verantwortliche die betroffene Person vor einer Aufhebung der Einschränkung zu unterrichten.

(4) Der Verantwortliche hat die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder eine Einschränkung der Verarbeitung sowie über die Gründe für die Verweigerung zu unterrichten. Der Verantwortliche hat die betroffene Person auch über die Möglichkeit zu unterrichten, bei der Datenschutzbehörde Beschwerde einzulegen.

(5) Der Verantwortliche hat die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde mitzuteilen.

(6) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß Abs. 1 bis 3 hat der Verantwortliche alle Empfänger der betroffenen personenbezogenen Daten in Kenntnis zu setzen. Die Empfänger sind verpflichtet, die in ihrer Verantwortung liegenden personenbezogenen Daten unverzüglich zu berichtigen, löschen oder deren Verarbeitung einzuschränken.“[160]

[160] § 45 DSG

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.1.1.6 Kritik des Rechtes auf Vergessenwerden

In diesem Zusammenhang stellt sich die Frage, ob durch das Recht auf Vergessenwerden andere Grundrechte, wie die Meinungs- und Pressefreiheit eingeschränkt werden. Weder die Meinungs- und Pressefreiheit noch das Recht auf Löschung sind absolute Rechte. Es muss ein Ausgleich gefunden werden und einzelfallbezogen beurteilt werden, ob das Rechts auf Löschen möglich ist (siehe Ausführungen im Punkt 4.1.1.4). In Bezug auf die Abwägung sind zwar Vorgaben im Urteil des EuGHs erwähnt, die Umsetzung ist aber für die Suchmaschinenbetreiber sicher eine Herausforderung, da sie dies nicht generalisieren können und immer auf den konkreten Fall eingehen müssen.

4.1.1.7 Max Schrems und Europe v. Facebook

Max Schrems ist ein österreichischer Jurist und Datenschutzaktivist. Im Jahr 2012 gründete er den **Verein zur Durchsetzung des Grundrechts auf Datenschutz "europe-v-facebook.org"** (Europe versus Facebook). Wesentliches Ziel von Schrems ist, das Recht auf Datenschutz, welches auf Europarechtsebene verankert wurde, durchzusetzen. Der Verein zur Durchsetzung des Grundrechtes auf Datenschutz ist nicht auf Gewinn ausgerichtet und hat die aktive rechtliche Durchsetzung des Grundrechts auf Datenschutz, die nötige begleitende Information und Medianarbeit sowie politische Aufklärung als Zweck.[161] Es sollen Musterverfahren gegen Unternehmen, die das Grundrecht auf Datenschutz potentiell gefährden, unterstützt werden.[162] Obwohl es sich bei seinen Aktivitäten nicht um die Verankerung des Rechtes auf Vergessenwerden geht, muss man die Arbeit von Schrems näher erläutern, da sie mit dem Recht auf Löschung von Daten im Zusammenhang steht.

Am 25. Juni 2013 legte Schrems eine Beschwerde beim Commissioner in Irland ein, mit der er ihn im Wesentlichen aufforderte, Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die Vereinigten Staaten zu untersagen. Er machte geltend, dass das Recht und die Praxis der Vereinigten Staaten keinen ausreichenden Schutz gewährleisteten, weil die in diesem Land

[161] Entscheidung des OGH vom 20.07.2016, GZ 6 Ob 23/16z (2016): 4
[162] Entscheidung des OGH vom 20.07.2016, GZ 6 Ob 23/16z (2016): 4

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

gespeicherten personenbezogenen Daten den Überwachungstätigkeiten der Behörden ausgesetzt sind. Dabei verwies er auf die von Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der Vereinigten Staaten, insbesondere der National Security Agency (NSA).[163]

Der Commissioner wies die Beschwerde von Schrems als unbegründet zurück. Schrems erhob gegen diese Entscheidung eine Klage beim High Court, welche die Rechtsfrage dem EuGH vorlegte. Der EuGH entschied darauf in der Rechtssache C-362/14[164] Maximilian Schrems gegen Data Protection Comissioner, dass das „Safe-Harbor-Abkommen" zwischen EU und USA ungültig ist. Es wurde im Wesentlichen festgestellt, dass die USA kein angemessenes Datenschutzniveau gewährleistet und das Safe-Harbor-Abkommen nicht die Anforderungen eines effektiven Grundrechtschutzes erfüllt.[165]

Die wichtigsten Feststellungen aus dem Urteil kann man wie folgt zusammenzufassen:[166]

1. Die Grundrechte verpflichten die Kommission dazu, in Verhandlungen mit Drittstaaten ein bestimmtes Mindestschutzniveau nicht zu unterschreiten.[167]

2. Für eine datenschutzrechtliche Entscheidung der Kommission gilt zwar die Vermutung der Rechtmäßigkeit, die von den Aufsichtsbehörden nicht in

[163] EuGH vom 06.10.2015, C-362/14, InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020)
[164] EuGH vom 06.10.2015, C-362/14, InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020)
[165] Thomas Petri. „Die Safe-Harbor Entscheidung." Datenschutz und Datensicherheit – DuD Ausgabe 12/2015 (2015): 803-804
[166] Thomas Petri. „Die Safe-Harbor Entscheidung." Datenschutz und Datensicherheit – DuD Ausgabe 12/2015 (2015): 803-804
[167] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 73, 78

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

eigener Kompetenz für ungültig erklärt werden kann, weil eine solche Kompetenz nur dem EuGH zusteht.[168]

3. Eine Angemessenheits-Entscheidung der Kommission kann die Kontrollpflichten der mitgliedstaatlichen Datenschutzbehörden nicht beschränken.[169]

4. Die Datenschutz-Aufsichtsbehörden müssen mit Kompetenzen ausgestattet werden, die ihnen eine effektive Sachverhaltsaufklärung und Einwirkungsmöglichkeiten ermöglichen. Die Mitgliedstaaten sind im Anwendungsbereich der Charta der Grundrechte verpflichtet ein Klagerecht der Aufsichtsbehörden vorzusehen.[170]

5. Die Entscheidung der Kommission ist einseitig, da sie den Sicherheitserfordernissen der USA Vorrang gegenüber den Grundrechten der EU-Bürgerinnen und -Bürger einräumt. Auch aus Gründen der inneren Sicherheit darf der Schutz des Grundrechts auf Achtung des Privatlebens nur im absolut notwendigen Maß eingeschränkt werden.[171]

6. Aus der Ungültigkeit der Entscheidung folgt nicht zwingend, dass die USA nicht auch ein angemessenes Datenschutzniveau gewährleisten könnten.

---

[168] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 52, 62
[169] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 53
[170] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 65
[171] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 82, 86, 87, 92

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

7. Ein angemessenes Schutzniveau ist stets zu verneinen, wenn die betroffenen Personen keine Möglichkeit eines effektiven gerichtlichen Rechtsbehelfs haben.[172]

Da durch die Klage das Safe-Harbor-Abkommen außer Kraft gesetzt wurde, mussten die EU und USA ein neues Abkommen, das Privacy Shield, verhandeln. Dieses wurde mittlerweile von Schrems bekämpft und vom Europäischen Gerichtshof ebenso für ungültig erklärt (siehe Details im Kapitel 4.1.1.8).

Außer dem Verfahren vor dem EuGH hat Schrems eine Klage gegen das irische Tochterunternehmen von Facebook bei dem zuständigen Gericht in Wien eingebracht. Mit dieser Klage will Schrems erreichen, dass Facebook rechtskonform agiert und machte Unterlassungs- sowie Schadenersatzansprüche geltend. Weiters hat er die Facebook-Nutzer aufgerufen, sich dem Verfahren mit einer Sammelklage anzuschließen und ihre Forderungen ihm als Hauptkläger via „Abtretungs-App" abzutreten.[173] Über die von Max Schrems eingerichtete Webseite www.fbclaim.com haben mehr als 25.000 Verbraucher aus verschiedenen Länder dies getan.[174]

Das Landesgericht für Zivilrechtssachen in Wien, hat diese Klage in ersten Rechtsgang zurückgewiesen, mit der Begründung, dass das Gericht nicht zuständig ist. Diese Entscheidung wurde von Schrems bekämpft. Das Oberlandesgericht Wien hat als zweite Instanz entschieden, dass das angerufene Gericht zuständig ist. Weiters hat das Oberlandesgericht Wien entscheiden, dass der Kläger bei der Sammelklage keine weitere Privatnutzer vertreten kann und erlaubte zu diesem Punkt einen ordentlichen Revisionsrekurs, da es zur Frage einer „internationale Sammelklage" keine Rechtsprechung des OGH gibt.[175] Dies würde bedeutet, dass jeder Facebook Nutzer eigenständig klagen muss.

---

[172] InfoCuria. "C362/14 – Schrems" http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14 (zugegriffen 10.10.2020): 95

[173] Europe v Facebook. „Sammelklage gegen Facebook eingebracht." http://www.europe-v-facebook.org/sk/pa_de.pdf (zugegriffen 9.9.2020)

[174] Europe v Facebook. „Sammelklage gegen Facebook eingebracht." http://www.europe-v-facebook.org/sk/pa_de.pdf (zugegriffen 9.9.2020)

[175] Europe v Facebook. „Oberlandesgericht Wien entscheidet, Kläger ist ein Verbraucher." http://www.europe-v-facebook.org/PA_OLG_de.pdf (zugegriffen: 9.9.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Schrems stützt seine Klage primär auf dem Verbrauchergerichtsstand (Art 16 Abs 1 zweiter Fall EuGVVO alt). In der Klage wurde von Schrems vorgebracht, dass sieben weitere Nutzer vom Facebook, die in Österreich, Deutschland und Indien wohnten, ihre Ansprüche Schrems zediert haben.[176]

Der OGH hat die Frage der Zulässigkeit einer Sammelklage in Österreich gegen Facebook dem Europäischen Gerichtshof vorgelegt und im Wesentlichem zwei Fragen gestellt:

> *„Ist Art 15 EuGVVO VO (EG) Nr 44/2001 dahin auszulegen, dass ein „Verbraucher" im Sinne dieser Bestimmung diese Eigenschaft verliert, wenn er nach längerer Nutzung eines privaten Facebook-Kontos im Zusammenhang mit der Durchsetzung seiner Ansprüche Bücher publiziert, teilweise auch entlohnte Vorträge hält, Webseiten betreibt, Spenden zur Durchsetzung der Ansprüche sammelt und sich die Ansprüche von zahlreichen Verbrauchern gegen die Zusicherung abtreten lässt, diesen einen allfälligen Prozesserfolg nach Abzug der Prozesskosten zukommen zu lassen?"*[177]

> *„Ist Art 16 EuGVVO VO (EG) Nr 44/2001 dahin auszulegen, dass ein Verbraucher in einem Mitgliedstaat gleichzeitig mit seinen eigenen Ansprüchen aus einem Verbrauchergeschäft am Klägergerichtsstand auch gleich gerichtete Ansprüche anderer Verbraucher mit Wohnsitz a. im gleichen Mitgliedstaat, b. in einem anderen Mitgliedstaat oder c. in einem Drittstaat geltend machen kann, wenn ihm diese aus Verbrauchergeschäften mit derselben beklagten Partei aus demselben rechtlichen Zusammenhang zediert wurden und wenn das Zessionsgeschäft nicht in eine gewerbliche oder berufliche Tätigkeit des Klägers fällt, sondern der gemeinsamen Durchsetzung der Ansprüche dient?"*[178]

---

[176] Entscheidung des OGH RS0130905. GZ 6 Ob 23/16z. (20.07.2016)
[177] Entscheidung des OGH RS0130905. GZ 6 Ob 23/16z. (20.07.2016): 2
[178] Entscheidung des OGH RS0130905. GZ 6 Ob 23/16z. (20.07.2016): 2

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Der Europäische Gerichtshof hat entschieden, dass Schrems nicht als Zessionar von Ansprüchen anderer Verbraucher den Verbrauchergerichtsstandort in Anspruch nehmen kann, um die abgetretenen Ansprüche geltend zu machen.[179]

In der Sache selbst liegt noch keine rechtskräftige Entscheidung vor. Das Landesgericht für Zivilrechtssachen in Wien entschied, dass Schrems einen Schadenersatz in der Höhe von 500 Euro erhält, weil Facebook die Auskunftspflicht über sämtliche personenbezogene Daten verletzt habe. Schrems ist mit diesem Urteil nicht zufrieden und geht in Berufung.[180]

4.1.1.8 Das Privacy Shield Abkommen

Im Februar 2016 haben sich die EU und die USA auf neue Regeln zum Datenaustausch geeinigt, welches am 01.08.2016 unter dem Namen **„Privacy Shield" Abkommen** in Kraft getreten ist.

Diese Abkommen regelte die Übermittlung von Daten aus der EU in die USA. Nach dem Abkommen haben Unternehmen in der USA die Möglichkeit gehabt, sich in eine vom US-Handelsministerium geführten Liste („Privacy Shield List") eintragen zu lassen, wenn sie sich verpflichten die vereinbarten Anforderungen („Privacy Shield Principles") einzuhalten.[181]

Der Europäische Gerichtshof (EuGH) hat am 16. Juli 2020 das EU-US Privacy Shield mit sofortiger Wirkung für ungültig erklärt. Der EuGH begründete das Urteil damit, dass aufgrund der in den USA vorherrschenden Überwachungsprogramme und den daraus resultierenden Eingriffen in die Grundrechte der betroffenen Personen, das Datenschutzniveau der EU nicht

---

[179] Gerichtshof der Europäischen Union. „Pressemitteilung Nr. 7/18." https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-01/cp180007de.pdf (zugegriffen: 01.11.2020)

[180] ZackZack.at. „6 JAHRE NACH SCHREMS-KLAGE.„ https://zackzack.at/2020/07/01/6-jahre-nach-schrems-klage-facebook-urteil-veraergert-datenschuetzer/ (zugegriffen: 01.11.2020)

[181] WKO.at. „EuGH: EU-US Privacy-Shield ungültig." https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-US-Privacy-Shield.html (zugegriffen: 29.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

eingehalten werden kann. Es gibt auch keine Schutzmaßnahmen oder Garantien gegen solche Eingriffe in Bezug auf Daten, die unter dem Privacy Shield Abkommen ausgetauscht werden. Bezüglich der Standarddatenschutzklauseln hielt der EuGH fest, dass diese grundsätzlich gültig bleiben.[182]

Bei den Standarddatenschutzklauseln handelt es sich um Klauseln, die von der Europäischen Kommission erlassen wurden und ohne weitere Genehmigung durch die Aufsichtsbehörden als Grundlage für Datenübermittlungen in Drittländer genutzt werden können.[183] Die Standarddatenschutzklauseln sind auf der Website[184] der Europäischen Kommission abrufbar.

Über die Standarddatenschutzklauseln hinaus, können Daten in Drittländern auch aufgrund Angemessenheitsbeschlüsse sowie auf Grundlage der ausdrücklichen Einwilligung des Betroffenen übermittelt werden.[185]

Durch einen Angemessenheitsbeschluss der Europäischen Kommission wird festgelegt, dass ein Drittland ein angemessenes Schutzniveau für personenbezogene Daten bietet.[186] Eine Liste der Angemessenheitsbeschlüsse ist auf die Website[187] der Europäischen Kommission veröffentlicht.

---

[182] WKO.at. „EuGH: EU-US Privacy-Shield ungültig“, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-US-Privacy-Shield.html (zugegriffen: 29.10.2020)

[183] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. „Internationaler Datentransfer.“ https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Internationaler_Datentransfer.html (zugegriffen: 29.10.2020)**:** Standarddatenschutzklauseln

[184] European Commision. „Standard Contract Clauses (SCC).“ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. (zugegriffen: 29.10.2020)

[185] WKO.at. „EuGH: EU-US Privacy-Shield ungültig“, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-US-Privacy-Shield.html (zugegriffen: 29.10.2020)

[186] Der Europäische Datenschutzbeauftragte. „Glossary.“ https://edps.europa.eu/data-protection/data-protection/glossary/a_de (zugegriffen: 29.10.2020): Angemessenheitsbeschluss

[187] European Commision. „Adequacy decisions” https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (zugegriffen: 29.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.2 Technische Aspekte

Technisch gesehen ist die Möglichkeit des zentralen Löschens von Daten eine nicht triviale Aufgabe. Dies ist primär der dezentralen Architektur des Netzes geschuldet. Der technische Vorteil, der es jeden Menschen erlaubt, Daten sowie Services in einem globalen Netzwerk zur Verfügung zu stellen, bedingt auch, dass es keine zentrale Stelle gibt, die kontrollieren könnte, welche Daten, wann von wem gespeichert oder gelöscht werden, beziehungsweise welche Software eingesetzt werden muss um Daten zentral löschen zu können.[188] In den nächsten Kapiteln wird auf die technischen Herausforderungen sowie mögliche technologische Ansätze näher eingegangen.

4.2.1 Technische Herausforderungen

Die technischen Herausforderungen in Bezug auf das Löschen von Daten in einem verteilten, offenen Netzwerk sind vielfältig:

- Kopien

  Wenn Daten von einer Festplatte gelesen werden, befindet sich die erste Kopie der Daten bereits im Speicher. Die originalen Daten werden in diesem Fall weder geändert oder gelöscht, noch gibt es eine Referenz auf diese originalen Daten. Gleiches passiert auch, wenn eine Webseite aufgerufen wird. Daten, die lokal auf einem Server gespeichert werden, müssen immer wieder kopiert werden (Speicher, Netzwerk, Browser des Anwenders, …) bis sie in einem letzten Schritt dem Benutzer im Browser angezeigt werden können. Die meisten dieser Kopien sind temporär und werden schnell wieder verworfen, manche bleiben hingegen länger bestehen. Ein gutes Beispiel hierfür ist der temporäre lokale Speicher des Browsers, welcher in den meisten Fällen noch nach Monaten gewisse Daten auf dem lokalen Computer behält.[189]

---

[188] Preston Gralla, and Michael Troller. How the Internet Works, Eighth Edition. Eigth ed. Que, O'Reilly Media, (2006): Chapter 4. How the World Wide Web Works,

[189] Ilya Grigorik, High Performance Browser Networking, O'Reilly Media, (2013): 13. Optimizing Application Delivery

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Sicheres Löschen

Was bedeutet sicheres Löschen in der Cloud? Diese Frage ist an sich bereits technisch gesehen komplex, da die meisten Cloud-Provider nur sehr abstrahierte Speichertechnologien für ihre Anwender anbieten. Diese Technologien basieren in den meisten Fällen auf Basis von magnetischen Festplatten (Solid-State Speicher - SSD) oder magnetischen Bändern. Da der Benutzer keinen direkten Zugriff auf diese Systeme hat, kann der Anwender nicht verifizieren, ob die Daten wirklich auf diesen Speichern gelöscht wurden. Praktisch ist es möglich, Daten auf Speichermedien, die nicht oft genug überschrieben wurden, wiederherzustellen.[190]

- Auffinden von Daten

Durch die einfachen Möglichkeiten Daten zu kopieren, ist es für Anwender oft schwer alle Daten aufzufinden, die gelöscht werden sollen. Oft ist ein zentraler Datenkatalog nicht verfügbar, der dies vereinfachen würde.[191]

- Authentifizierung (Authentication)

Um sicherstellen zu können, dass auf Daten, die in der Cloud oder auch auf anderen Systemen gespeichert werden, nur Personen mit Zugangsberechtigung zugreifen, ist die Feststellung der Identität (Authentifizierung) notwendig. Über die Jahre hat sich besonders Kerberos[192] als eine weit verbreitete Lösung etabliert, diese kann jedoch nicht auf neue Webtechnologien angewendet werden, welche die Grundlange für die Cloud bilden.

---

[190] Gutmann, Peter. "Secure deletion of data from magnetic and solid-state memory." Proceedings of the Sixth USENIX Security Symposium, San Jose, CA. Vol. 14. (1996) 77—89

[191] Tony Baer, “Finding the data buried in cloud storage” https://www.zdnet.com/article/finding-the-data-buried-in-cloud-storage/ (zugegriffen: 10.09.2020)

[192] Kohl, John T. "The use of encryption in Kerberos for network authentication." Conference on the Theory and Application of Cryptology. Springer, New York, NY, (1989): 35–43.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Bereits 1997 hat Albert Reich ein Patent für "HTTP distributed remote user authentication system"[193] eingereicht.

Das heute am weitesten verbreiteten Protokoll für Authentifizierung im Web ist OpenID[194], ein offener Standard der OpenID Foundation[195]. Um dieses Service zu benützen, muss man einen Account bei einem OpenID Provider besitzen. Viele der heutigen Cloud-Provider (z.B.: Google, WordPress, Yahoo oder PayPal) verwenden bereits dieses Protokoll bzw. unterstützen es, so dass andere Applikationen und Plattformen die Authentifizierung ihrer Benutzer über OpenID durchführen können.

Seit einiger Zeit gibt es eine neue Initiative für die Web Authentication (WebAuthn)[196]. Hierbei handelt es sich um einen neuen W3C Standard der von vielen großen Cloud-Providern (z.B. Google, Microsoft) unterstützt wird, um einen einheitlichen Authentifizierungsstandard in Webbrowsern zu ermöglichen.

Erschwerend kommt hinzu, dass viele Aktionen nicht direkt durch den Benutzer in einem Browser, sondern über APIs oder Services, die auf die Cloud-Services zugreifen, durchgeführt werden. Oft steht nur indirekt ein Benutzer hinter der auszuführenden Aktion bzw. der Benutzerkontext ist nicht überall vorhanden. Insofern müssen auch Services eigene Authentifizierungsmethoden erhalten.

- Autorisierung (Authorization)

Nachdem sichergestellt wurde, dass es sich um eine gewisse Person handelt, diese authentifiziert wurde, muss festgestellt werden, welche Berechtigungen dieser Benutzer hat. In Bezug auf das Löschen von Daten muss überprüft werden, ob die Person die Aktion (Löschen aber auch das Erstellen von neuen

---

[193] Reiche, Albert. "Http distributed remote user authentication system." U.S. Patent No. 6,092,196. 18 Jul. 2000.

[194] Recordon, David, and Drummond Reed. "OpenID 2.0: a platform for user-centric identity management." Proceedings of the second ACM workshop on Digital identity management. (2006): 11-16

[195] OpenID. „OpenID Foundation." https://openid.net/foundation/ (zugegriffen: 1.2.2020)

[196] W3C. „Web Authentication: An API for accessing Public Key Credentials" https://www.w3.org/TR/webauthn/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Daten) durchführen darf oder nicht. Es bedeutet nicht notwendigerweise, dass die Person der Ersteller oder der Eigentümer dieser Daten ist. Um sicherzustellen, dass diese Berechtigungen erweiterbar sind, wurde bereits sehr früh ein Role-Based Access Control Model[197] eingeführt.

In der Cloud können diese Role-Based Access Modelle nicht direkt verwendet werden und müssen durch neue Technologien erweitert werden. Hierfür haben sich zwei Standards durchgesetzt, welche ein sogenanntes „Principal" definieren. Dieses Principal beschreibt, welche Aktionen eine authentifizierte Person durchführen darf.

Security Assertion Markup Language (SAML) [198] ist der älteste Standard der bereits 2001 vom der OASIS Konsortium definiert wurde und seit 2005 in seiner letzten Version (V2.0) vorliegt. SAML bietet beides, Authentifizierung und Autorisierung in einem Standard an. Dadurch können vor allem Unternehmen profitieren, die Single Sign-on (SSO) [199] Anforderungen umsetzten möchten.

OAuth2[200] ist im Gegenzug ein reiner Autorisierungsstandard. Er bildet gemeinsam mit OpenID die Basis für OpenID connect[201]. OAuth2 bietet die Möglichkeit eine Applikation im Namen eines Benutzers zu autorisieren. Damit hat die Applikation die Möglichkeit, Aktionen im Auftrag von dem Benutzer durchzuführen.

OAuth2 bzw. OpenID connect ist auch jenes Protokoll-das von den meisten Cloud-Providern (Google, Amazon, Microsoft, Facebook) bereits heute unterstützt wird.

---

[197] Sandhu, Ravi S., et al. "Role-based access control models." *Computer* 29.2 (1996): 38-47

[198] Oasis. „SAML v2.0 Errata" http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0-cd-02.html (zugegriffen: 1.2.2020)

[199] Celesti, Antonio, et al. "Three-phase cross-cloud federation model: The cloud sso authentication." 2010 Second International Conference on Advances in Future Internet. IEEE, 2010.

[200] „OAuth 2.0" https://oauth.net/2/ (zugegriffen: 1.2.2020)

[201] OpenID. „OpenID Connect" https://openid.net/connect/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Datenformate

Es gibt zahlreiche unterschiedliche Datenformate mit denen Cloud-Applikationen umgehen müssen. Normalerweise werden von Web-Plattformen wie Facebook, Twitter, WhatsApp oder Instagram nur eine kleine Auswahl an Formate unterstützt. Generell ist aber davon auszugehen, dass Benutzer unterschiedliche Arten von Daten auf Systemen abspeichern möchten. Diese Formate haben sehr unterschiedliche Eigenschaften.

Einige bringen bereits Sicherheitskonzepte mit sich - wie zum Beispiel das Portable Document Format (PDF), welches es ermöglicht, den Inhalt des Dokuments zu verschlüsseln. Durch diese Funktionalität können auch Einschränkungen definiert werden, die es dem Benutzer nicht erlauben, das Dokument zu drucken oder Inhalte zu kopieren. Um dies auf allen Plattformen zu ermöglichen, muss aber auch sichergestellt werden, dass alle Anwendungen, die dieses Dateiformat öffnen können, diese Funktionen unterstützten.

Andre Formate, wie beispielsweise das sehr weit verbreitete Text Format (TXT) oder auch JPEG bieten keine Möglichkeit an, den Inhalt der Datei zu schützen.

Natürlich kann jede Datei nachträglich verschlüsselt werden. Dies bringt jedoch weitere Herausforderungen mit sich, da diese Dateien nur sehr schwer weiterverarbeitet werden können, erst dann, wenn sie wieder entschlüsselt wurden.

- Meta-Informationen

In den allermeisten Fällen ist es notwendig, dass Cloud-Systeme nicht nur Daten speichern und Anwendern wieder zur Verfügung stellen, sondern auf Basis der Daten weitere Informationen generieren. Instagram[202] beispielsweise verwendet die Fotos nicht nur um sie anderen Benutzern anzuzeigen, es zieht daraus auch Informationen, um ihre Benutzer bessere Inhalte anbieten zu können (z.B.: Bilderkennung, Hashtags). Diese Meta-Informationen über die Daten beziehungsweise über die Benützung der Services werden in den meisten Fällen unabhängig von den jeweiligen Daten gespeichert. Technisch besteht

[202] Instagram. „Instagram.“ https://www.instagram.com/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

auch hier keine direkte Verbindung zu den Daten. Trotzdem sollten Metadaten auch mit den Originaldaten gelöscht werden.

- Latenz

In einem global verteilten System spielt Latenz[203] eine wichtige Rolle. In welcher Zeit eine Löschoperation umgesetzt werden muss beziehungsweise werden kann, hängt sehr von der Architektur der Systeme ab. Speziell in weltweit verteilten Systemen kann es hier durchwegs zu mehrere Sekunden Verzögerung kommen. Werden Caching-Technologien eingesetzt, kann sich dies bis zu einigen Tagen erhöhen.

- Technologiebruch

So gut wie nicht zu kontrollieren ist das Löschen oder Kopieren von Daten, wenn es zu einem Bruch des Mediums kommt. Ein einfaches Beispiel hierfür ist das Abfotografieren eines Inhaltes oder eines Bildschirms. Auch wenn Betriebssysteme das Abfotografieren mittels Screenshots verhindern können, gibt es immer die Möglichkeit, dies mittels eines anderen Gerätes zu tun.

4.2.2 Existierende Technologien

In den folgenden Kapiteln wird eine Übersicht über existierende Technologien geben, welche das Problem des Löschens von Daten aus unterschiedlichen Blickwinkeln betrachten beziehungsweises dafür verwendet werden können Teile der Anforderungen zu erfüllen.

[203] Coulouris, George F., Jean Dollimore, and Tim Kindberg. Distributed systems: concepts and design. pearson education, 2005.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.2.2.1 X-pire!

X-pire! wurde erstmals 2001 in einem Paper „X-pire! – A digital expiration date for images in social networks“ [204] vorgestellt. In diesem Paper widmen sich die Autoren einem System, welches es ermöglicht, Bilder ein Ablaufdatum im Internet zu geben. Im speziellen wollen die Autoren das Veröffentlichen auf sozialen Netzwerken sicherer gestalten. Hierzu werden die Bilder durch einen symmetrischen Schlüssel, welcher in einer zentralen Datenbank gespeichert wird, verschlüsselt. Der Zugriff auf den Schlüssel wird nur bis zum Ablaufdatum der jeweiligen Datei gewährt. Nachdem das Bild verschlüsselt wurde, werden die Daten auf einem Server gespeichert. Um das Bild wieder herstellen zu können, muss die verschlüsselte Datei sowie der Schlüssel vom Server empfangen werden. Danach kann der Client das originale Bild wiederherstellen.

Die Verschlüsselung von Bildern, welche im Internet meist in dem sehr verbreiteten JPEG Format gespeichert und ausgeliefert werden, birgt einige Herausforderungen mit sich. Die meisten Plattformen speichern nicht die originalen Bilder, sondern wenden eigene Optimierungen auf den Bildern an. Sehr häufig werden Bilder neu codiert, um eine bessere Komprimierung zu erzielen, oft werden aber auch Metainformationen gelöscht oder eingefügt. Um Dateien beim Hochladen nicht sofort zu zerstören, verwendet X-pire! einen Mechanismus, der auch mit komprimierten Bildern umgehen kann. Die Abbildung 10 zeigt den genauen Ablauf den X-pire! verwendet, um die Daten zu verschlüsseln und dem Provider zur Verfügung zu stellen.

[204] Backes, Julian, et al. "X-pire!-a digital expiration date for images in social networks." arXiv preprint arXiv:1112.2649 (2011).

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

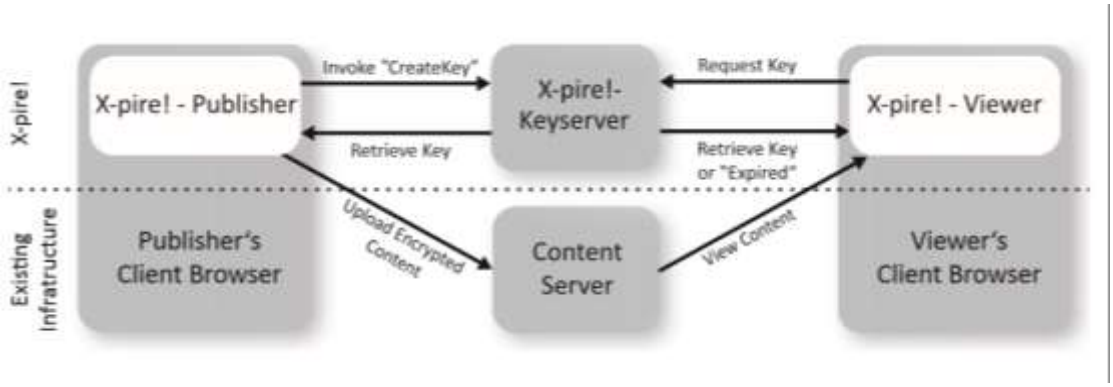

Abbildung 10: X-pire! Architektur [205]

Wie bereits weiter oben erwähnt, hat sich X-pire! auf JPEG Format fokussiert. Das JPEG[206] Format wurde 1992 von der Joint Photographic Experts Group entwickelt und stellt seit damals den Standard dar, Bilder komprimiert im Internet auszuliefern. Der Grund für X-pire! sich auf diesen Standard zu beziehen, liegt in zwei Bereichen. Erstens ist dieses Format im Internet sehr stark verbreitet, zweitens bietet es, im Gegensatz zu vielen anderen Formaten, die Möglichkeit, zusätzliche Informationen abzulegen, sowie unterschiedliche Transformationen zu unterstützen.

Generell verwendet X-pire! eine zentrale Infrastruktur (X-pire! - Keyserver) welcher die Verschlüsselung sowie die Auslieferung der notwendigen Schlüssel übernimmt. Dieser zentrale Ansatz wurde absichtlich gewählt, um die Möglichkeit von Angriffen auf das System zu reduzieren. Der zentrale Ansatz bietet durch die Möglichkeit Schlüsselanfragen von IP-Adressen auf Basis ihrer Häufigkeit und Art zu reduzieren, sowie zusätzliche Sicherheitsmaßnahmen einzuführen (z.B. Captchas[207]) bevor das Bild selbst geladen wird, einige Vorteile.

---

[205] Backes, Julian, et al. "X-pire!-a digital expiration date for images in social networks." arXiv preprint arXiv:1112.2649 (2011).

[206] CCITT. „INFORMATION TECHNOLOGY – DIGITAL COMPRESSION AND CODING OF CONTINUOUS-TONE STILL IMAGES – REQUIREMENTS AND GUIDELINES“ http://www.w3.org/Graphics/JPEG/itu-t81.pdf (zugegriffen: 1.3.2020)

[207] Chew, Monica, and J. Doug Tygar. "Image recognition captchas." International Conference on Information Security. Springer, Berlin, Heidelberg, (2004) 268--279

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Fazit:

X-pire! ist ein System, welches es erlaubt JPEG Bilder zu verschlüsseln und mit einem Ablaufdatum zu versehen. Diese Bilder können dann in unterschiedlichen sozialen Netzwerken (z. B. Facebook, Flicker) gespeichert werden. So lange der X-pire! Server diese Bilder als gültig erklärt, können sie, ohne die Notwendigkeit zusätzliche Software auf einem Computer oder in einem Browser zu installieren, direkt abgerufen werden. X-pire! erlaubt es auch, zusätzliche Sicherheitsmechanismen (IP – Filtering, - Drosselung, Captchas) einzuführen.

Aus Sicht einer generellen Lösung für das Internet hat X-pire! einige Schwachstellen. In erster Linie ist es nur für JPEG Bilder geeignet. Dies ist für Social Media Anwendungen durchaus ein sehr relevanter Teil an Informationen, die verbreitet werden, es ist aber schwer vorstellbar, dass das gleiche System auch auf Text oder andere Arten von Dokumenten (z.B. Videos) angewendet werden kann, da es spezielle Möglichkeiten des JPEG Formates nützt, welche in vielen anderen Formaten nicht enthalten sind.

Betrachtet man ausschließlich die Absicherung von Bildern, kann durch X-pire! auch nicht ausgeschlossen werden, dass Angreifer, die das Bild einmal erfolgreich geöffnet haben, dieses nicht unverschlüsselt speichern bzw. weiterverbreiten. Eine andere Möglichkeit wäre es, durch spezielle Software (Malware)[208] alle notwendigen Schlüssel von dem X-pire! Server lokal zu speichern, wodurch Bilder auch nach Ablauf trotzdem entschlüsselt werden können. Dieser Ansatz könnte, wie die Autoren beschreiben, durch erhöhte Sicherheitsmaßnahmen (IP – Filterung, Captchas) erschwert werden. Durch neue Technologien ist es jedoch nicht sehr schwierig diese zu umgehen. IP – Filterung kann durch Public Cloud-Services umgangen werden, indem die verwendeten Rechner immer wieder gewechselt werden. Andererseits ist es in den letzten Jahren auch einfacher geworden Capture automatisch[209] oder semiautomatisch[210] zu entschlüsseln.

---

[208] Hannes, Federrath, Karl-Peter Fuchs, Dominik Herrmann, Daniel Maier, Florian Scheuer, und Kai Wagner. „Grenzen des digitalen Radiergummis.“ Datenschutz und Datensicherheit - DuD 35 (2011): 403-407

[209] Saini, Baljit Singh, and Anju Bala. "A review of bot protection using captcha for web security." IOSR Journal of Computer Engineering 8.6 (2013): 36-42.

[210] Balaban, D, “Understanding CAPTCHA-solving services in an economic context” (2011): 3: evaluation of the human-based services

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.2.2.2 X-pire 2.0

Aufbauend auf dem ursprünglichen X-pire! System wurde 2014 eine Verbesserung dieses vorgestellt[211].

Die Autoren des erweiterten Systems hatten vier Ziele, die sie adressieren wollten:

1) Personen die vollständige Kontrolle über geteilte Inhalte zu ermöglichen.
2) Das „Data Duplication Problem“ (DDP) zu lösen.

   Das DDP ergibt sich daraus, dass Anwender, welche einmal Zugriff auf ein Dokument erhalten haben, nicht daran gehindert werden, dieses Dokument unverschlüsselt zu speichern. Dies gilt nur für eine direkte Kopie der Daten, es kann natürlich nicht verhindert werden, dass jemand Inhalte von einem Monitor mittels Kamera abfotografiert.
3) Weiterhin eine einfache Integration in existierende Systeme wie Flicker oder Facebook zu ermöglichen.

Die größte Herausforderung und Neuerung gegenüber des ursprünglichen X-pire! Systems war es, das DDP zu lösen. Während X-pire! davon ausgeht, dass nur vertrauenswürdige Personen Zugriff auf die Daten gegeben wird, möchte X-pire 2.0 ausschließen, dass irgendjemand Daten lokal unverschlüsselt abspeichert. Dies ist insofern relevant, da in sozialen Netzen zwar meist die Möglichkeit besteht, den Zugriff auf Daten einer Person einzuschränken, dies jedoch im Internet generell nicht vorausgesetzt werden kann.

Um das DDP zu adressieren, muss sichergestellt werden, dass zu keinem Zeitpunkt der Schlüssel von Daten oder Daten in unverschlüsselter Form, abgespeichert werden. Trotzdem muss ein Weg gefunden werden, um sie anzuzeigen. In X-Pire 2.0 wird ein sogenanntes „Trusted Execution Environment“ (TEE)[212] eingeführt, welche es ermöglicht die Verschlüsselung sowie die Anzeige der Daten in einer gesicherten Umgebung durchzuführen. Diese Umgebung macht

---

[211] Backes, Michael, et al. "X-pire 2.0: a user-controlled expiration date and copy protection mechanism." Proceedings of the 29th annual ACM Symposium on applied computing. (2014): 1633--1640

[212] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: what it is, and what it is not." 2015 IEEE Trustcom/BigDataSE/ISPA. Vol. 1. IEEE, 2015.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

es Angreifern und potenzieller Schadsoftware unmöglich die Daten unverschlüsselt zu lesen.

Um Daten am Server auch sicher abzuspeichern und die Möglichkeit von Angriffen gering zu halten, wurde wie bereits bei X-pire! auf eine zentrale Infrastruktur gesetzt. Auch der Keyserver benötigt sichere Hardware, um eine mögliche Profilierung von User basierten Key-Anfragen zu verhindern.

Abbildung 11 beschreibt den genauen Ablauf, wie Daten publiziert und abgerufen werden. Das Publishing erfolgt sehr ähnlich zu dem X-pire! System, mit der Ausnahme, dass der Keyserver spezielle Sicherheitsanforderungen hat, um die Schlüssel zu speichern. Der primäre Unterschied liegt in der Entschlüsselung und Anzeige der Daten, welche in einer Trustzone durchgeführt wird. Das Konzept einer Trustzone wurde von ARM[213] entwickelt und bildet die Grundlage für X-pire 2.0.

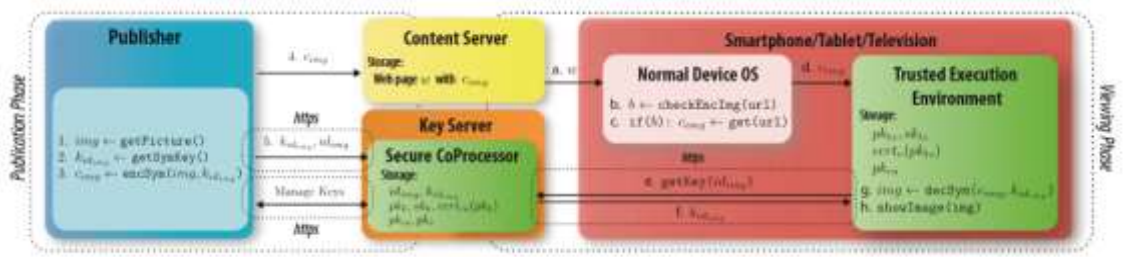

Abbildung 11: X-Pire 2.0 publizieren von Daten[214]

Die größte Herausforderung bei der Bildung der Trustzone ist es, wie die Bilder später auf dem Computerbildschirm angezeigt werden, da normalerweise Social Media Seiten über einen Browser oder App aufgerufen werden. Hier stellt X-Pire 2.0 drei Möglichkeiten vor.

[213] ARM. “Security technology building a secure system using trustzone technology” (2006)
[214] Backes, Michael, et al. "X-pire 2.0: a user-controlled expiration date and copy protection mechanism." Proceedings of the 29th annual ACM Symposium on applied computing. 2014. 1633--1640

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

1) Überblendung mittels Trustzone

   Hierfür wird ein Plugin für den Browser benötigt, welches immer, wenn ein geschütztes Bild geladen wird, dieses automatisch an den X-pire 2.0 Services in der Trustzone weiterleitet.

2) Browser wird in Trustzone betrieben

   Eine weitere Möglichkeit wäre es, den gesamten Browser in der Trustzone laufen zu lassen.

3) Wechseln zu der Trustzone

   In diesem Fall würden die Bilder nicht an ihrer eigentlichen Stelle im Browser angezeigt, stattdessen würde ein TZ Viewer die Bilder in der gesicherten Trustzone anzeigen. Für die Demo Implementierung wurde dieser Ansatz verwendet.

Fazit:

Generell ist zu sagen, dass X-Pire 2.0 primär das Data Duplication Problem versucht zu adressieren. Die vorgeschlagene Trustzone kann hier sicher eine erhöhte Sicherheit der Daten liefern, bringt aber gleichzeitig neue Herausforderungen.

Ebenso wie X-pire! adressiert X-Pire 2.0 derzeit nur Bilder und setzt auf das JPEG Protokoll. X-Pire 2.0 hat hier sicher Vorteile auch andere Dokumenttypen zu unterstützen, da es bereits davon ausgeht eine spezielle Software für die Anzeige in der Trustzone zu benötigen. Dies ist in der derzeitigen Form aber nicht vorgesehen. Genau dieser Aspekt birgt die größte Schwierigkeit mit sich. Benutzer müssen zusätzliche Software installieren, um die gesicherten Bilder anzuzeigen. Zusätzlich gibt es derzeit keine Lösung für die immer stärker werdenden Apps auf mobilen Endgeräten. Im Gegensatz zu den meisten Browsern, welche die Möglichkeit haben Erweiterungen zu installieren, um die vorgeschlagene Sicherheit zu erreichen, kann dies in den Applikationen nicht so einfach erfolgen. Anwender sind davon abhängig, dass Firmen wie Facebook oder Instagram die Funktion in ihre Anwendungen einbauen.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Auch der derzeit gewählte Ansatz, Bilder in einem separaten Anzeigeprogramm darzustellen, ist für die meisten Benutzer sicher nicht optimal. Speziell in sozialen Netzwerken, in denen primär Bilder und Videos geteilt werden, ist eine Zuordnung der Inhalte zu den Texten essenziell und mit diesem Ansatz nur sehr schwierig zu gewährleisten.

4.2.2.3 Vanish System

Vanish[215] beschreibt ein System, das es sich zum Ziel gesetzt hat, alle Kopien von Daten nach einer gewissen Zeit unlesbar zu machen. Die ursprüngliche Überlegung der Entwickler war es, das System auf die Archivierung von Daten (z.B. E-Mails) anzuwenden, um die Privatsphäre von vergangenen Informationen sicherzustellen. Im Gegensatz zu anderen Ansätzen (z.B. X-pire!) möchte Vanish sicherstellen, dass Daten, ohne eine spezielle Aktion des Users zu erfordern, automatisch nach einem benutzerspezifischen Ablaufdatum nicht mehr lesbar sein soll. Diese Zusicherung soll auch noch gültig sein, wenn ein Angreifer Zugriff auf die Daten, sowie den kryptographischen Schlüssel und das Passwort erlangt. Weitere Anforderungen an das Vanish System waren, dass es ohne spezielle sichere Hardware auskommt und keine zusätzlichen externen Services notwendig sind.

Um die Anforderungen umzusetzen, entschlossen sich die Entwickler kryptografische Verfahren mit einem verteilten selbst zerstörenden Datenspeicher zu kombinieren. Ein wichtiges Kriterium war es, einen nicht zentralen Datenspeicher zu verwenden, sondern auf ein P2P Netzwerk zu setzten. Dieser sich selbst zerstörende Datenspeicher ist die zentrale Komponente des Vanish Systems. Im Konkreten entschieden sich die Entwickler sogenannte Distributed Hash Tables (DHTs)[216] einzusetzen.

---

[215] Geambasu, Roxana, et al. "Vanish: Increasing Data Privacy with Self-Destructing Data." USENIX Security Symposium. Vol. 316. (2009)

[216] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Distributed Hash Tables (DHTs):

Wie der Name bereits vermuten lässt, handelt es sich bei DHTs um sehr robuste, verteilte Key-Value Datenbanken. Diese Datenbanken werden durch ein P2P Netzwerk verteilt. Es gibt einige Vorteile von DHTs die für das Vanish System von entscheidender Bedeutung sind:

1) Skalierbarkeit

   Mehr als 1 Million Knoten (wie im Falle von Vuze DHT[217]), welche geographisch über mehrere Länder verteilt sind, machen solche Systeme robust gegen unterschiedliche Arten von Angriffen.

2) Zuverlässigkeit

   DHTs sind dafür gebaut worden, um einen sehr zuverlässigen verteilten Speicher zu garantieren.[218, 219] Vanish verwendet dies, um sicherzustellen, dass die zu schützenden Daten auch wirklich für den bestimmten Zeitraum zugreifbar bleiben.

3) Churn

   Das Netzwerk und die darin gespeicherten Daten verändert sich konstant. Immer wieder werden neue Knoten in das P2P Netzwerk aufgenommen, um Daten zu speichern, wohingegen ältere Knoten das Netz verlassen. Die Lebensdauer der Knoten hängt sehr stark vom Netzwerk ab. Während sie

---

[217] Falkner, Jarret, et al. "Profiling a million user DHT." Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. 2007.

[218] Maymounkov, Petar, and David Mazieres. "Kademlia: A peer-to-peer information system based on the xor metric." International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002.

[219] Rowstron, Antony, and Peter Druschel. "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems." IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing. Springer, Berlin, Heidelberg, 2001.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

in Kazaa[220] nur wenige Minuten beträgt, sind es in Vuze/Azureus[221] mehrere Stunden. Dieser Churn ist in den meisten Anwendungsfällen eher unerwünscht, da es zu Verlust von Daten kommen kann. Genau diese Eigenschaft ist aber in Vanish essenziell.

DHTs sind nicht vollständige relationale Datenbanken, sondern ermöglichen es Key-Value Paare zu speichern. Um Daten zu adressieren, ist es notwendig den Schlüssel (Key) bereits zu kennen. Abhängig von diesem Schlüssel werden die Daten auf einen oder mehrere Knoten verteilt.

Möglichen Datenoperationen, die DHTs zur Verfügung stellen, variieren sehr stark. DHTs, die für Vanish relevant sind, bieten aber sehr ähnliche Datenoperationen an. Diese sind sehr einfach und erlauben das Speichern (put) und Lesen (get) von Daten sowie die Abfrage, welcher Knoten für einen gewissen Index zuständig ist.

Vanishing Data Object (VDO):

Um in unterschiedliche Applikationen die Möglichkeit von sich selbst zerstörenden Daten zu unterstützten, wurde von Vanish das Vanishing Data Object (VDO) eingeführt. Dieses Objekt kapselt den Inhalt (Text, Datei) und schützt unabhängig davon, ob das VDO kopiert, versendet oder im Internet öffentlich zum Download bereitgestellt wird davor, dass nicht endlos darauf zugegriffen werden kann. Die Daten liegen nicht in einem Format vor, welches direkt geöffnet werden kann. Damit stellt das Format sicher, das abgelaufene Daten nicht mehr abgerufen werden können.

Zusätzlich zu den geheimen Daten (C) enthält das VDO noch drei weitere Parameter, die für die Wiederherstellung essenziell sind. L bezeichnet eine Zufallszahl die notwendig für die Verschlüsselung ist, n die Anzahl der Einträge

[220] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160

[221] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

in dem DHT und k die Schwelle der notwendigen Knoten, um Daten wiederherzustellen.

Somit besteht VDO = {C, L, n, k}

Vanishing Algorithmus:

Um die Daten zu verschlüsseln generiert Vanish eine Zufallszahl, die für die Initialisierung eines pseudo Nummerngenerators verwendet wird. Die Aufgabe des pseudo Nummerngenerators ist es, deterministisch immer die gleichen Zahlen zu liefern, sofern er mit der gleichen Zufallszahl initialisiert wird.

```
Long L = 23456
Random rdn = new Random (L);
Int l1 = rdn.nextInt();
Int l2 = rdn.nextInt();
```

Folgendes Stück pseudo Code liefert damit immer, unabhängig davon, wo es ausgeführt wird, die gleichen Zahlen für l1, l2 und alle weiteren nextInt() Anfragen. Abhängig davon auf wie viele Indexe der verwendete Chiffre Schlüssel aufgesplittet werden soll. Als Nächstes wird der Shamir Secret Sahring Algorithmus verwendet, um den Schlüssel auf n Teile aufzuteilen. Diese werden danach in dem DHT unter den zuvor generierten Indizes gespeichert. Nachdem der Inhalt mit dem Schlüssel chiffriert wurde, generiert der Algorithmus ein VDO, welches sich aus dem verschlüsselten Daten, der Initialisierungsnummer für den Zufallsgenerator (L) sowie der notwendigen Shamir Secret Sharing Teile (k) für die Wiederherstellung der Daten zusammensetzt.

Das VDO kann daraufhin lokal gespeichert oder versendet werden. Gleichzeitig muss der Originalinhalt gelöscht werden.

Um den Inhalt wieder herstellen zu können, benötigt man nur das VDO, welches z.B. auf einem Server gespeichert werden kann. Nach dem Empfang des VDO erstellt der Leser wieder einen pseudo Zufallsgenerator, der durch die Zahl (L) im VDO initialisiert wird. Danach generiert der Leser die notwendigen n Indizes,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

unter welchen die Teile der Chiffre abgelegt wurden. Wenn mehr als die notwendigen k Teile gefunden wurden, kann der Shamir Secret Sharing Algorithmus den Schlüssel für die Entschlüsselung wiederherstellen und somit die Information gelesen werden. Sollten weniger als die notwendigen k Teile gefunden werden, ist der Inhalt nicht mehr lesbar.

Lebenszeit von VDOs:

Eine der Herausforderungen ist es, die Lebenszeit von VDOs zu erhöhen. Dies ergibt sich daraus, dass Systeme wie Vuze eine zu kurze Zeit für das Ablaufen der Daten haben. Sollen Daten länger erhalten bleiben, müssen die Schlüsselteile neu auf die unterschiedlichen Server verteilt werden. Hierfür können die gleichen Indizes verwendet werden. Dadurch ist sichergestellt, dass der Schwellwert an notwendigen Teilen nicht unterschritten wird. Vanish sieht hierfür eine Erneuerung alle acht Stunden vor. Dafür muss eine Verbindung zum DHT Netzwerk gegeben sein.

Mögliche Angriffe:

Einige Zeit nach Vorstellung des Vanish Systems wurden einige Schwachstellen[222] bekannt. Eine davon ist auf die Besonderheit des verwendeten Vuze DHT zurückzuführen. In diesem gibt es die Möglichkeit, dass ein neu hinzugefügter Knoten automatisch alle, in seinem Indexbereich zu speichernden Daten, von anderen Knoten gepushed bekommt. Durch diese Möglichkeit können Angreifer einfach und innerhalb von kürzester Zeit zu großen Mengen an Verschlüsselungsteilen kommen und diese lokal ablegen.

Eine Art einer solchen „Sybil-Attack“[223, 224] Angriffes ist eine so genannte „Hopping-Attack“. Eine Hopping-Attack nutzt die oben aufgezeigte Schwachstelle von Vuze DHT aus. Ein Angreifer erhält normalerweise die

---

[222] Geambasu, Roxana, et al. "Experiences building security applications on DHTs." technical report, UW-CSE-09–09–01 (2009).

[223] Douceur, John R. "The sybil attack." International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002.

[224] Cholez, Thibault, et al. "Detection and mitigation of localized attacks in a widely deployed P2P network." Peer-to-Peer Networking and Applications 6.2 (2013): 155-174.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Informationen seiner nächsten 20 Nachbarn. Durch diesen Mechanismus und die Möglichkeit eines Portwechsels schnell die Lokation innerhalb des P2P Netz zu wechseln, kann ein Angreifer innerhalb von sehr kurzer Zeit sämtliche Einträge lokal speichern.

Um diese Angriffsmethode zu verhindern, wurde ein weiteres DHT System vorgeschlagen, welches die Schwachstelle nicht besitzt (OpenHDT[225]). Die Schlüssel werden hierbei teilweise in beiden Netzwerken abgelegt. Dadurch würden sich die Kosten für einen erfolgreichen Angriff auf das Vanish System dramatisch erhöhen.

Safevanish:

Aufbauend auf den Schwachstellen von Vanish, wurden auch andere Möglichkeiten der Verbesserung aufgezeigt. Ein Ansatz biete das *Safevanish* System. Um eine „Hopping-Attack" zu erschweren, schlagen die Autoren vor, jeden Teilschlüssel des Shamir Secret Algorithm mit einer gewissen Anzahl an Bytes zu erweitern. Generell ist die Teilschlüssellänge sehr kurz (16 – 51 Bytes), wodurch es sehr einfach ist die Daten durch eine Attacke zentral zu speichern. Wenn die Schlüssel aber durch zufällige Daten erweitert wird, erhöht sich der Aufwand eines Angreifers enorm.[226]

Fazit:

Das Vanish System stellt eine skalierbare und auf sämtliche Datenformate anwendbare Plattform zur Verfügung, die es erlaubt Daten ein Ablaufdatum zu geben. Wie die Designer in ihrem Paper auch aufzeigen, gibt es viele Möglichkeiten das System in bestehende Applikationen einzubinden. Im

[225] Rhea, Sean, et al. "OpenDHT: a public DHT service and its uses." Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications. 2005.

[226] Zeng, Lingfang, et al. "Safevanish: An improved data self-destruction for protecting data privacy." 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE, 2010.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Konkreten wurden ein Firefox Plug-In[227] sowie eine Erweiterung für Gmail entwickelt, die es ermöglichen Texte zu verschlüsseln und mit einem Ablaufdatum zu versehen. Das Firefox Plug-In ist auch für soziale Netzwerke anwendbar, in dem das verschlüsselte VDO gepostet wird. Jeder der den Inhalt entschlüsseln möchte, kann dies innerhalb der vorgegebenen Zeit durch das Vanish System mittels Firefox Plug-In erreichen. Natürlich gibt es die Möglichkeit auch für andere Browser ähnliche Erweiterungen zur Verfügung zu stellen.

Eine Schwachstelle in Bezug auf soziale Netzwerke ist, dass im Gegensatz zu X-pire! Bilder nur sehr schwer verschlüsselt bzw. diese nicht im Kontext der Webseite angezeigt werden können.

Neben der Möglichkeit, Inhalte ein Ablaufdatum zu geben, adressiert Vanish sowie Securevanish nicht, was mit den bereits wiederhergestellten Daten passiert. In der derzeitigen Architektur ist nicht vorgesehen, dass diese nicht lokal gespeichert, bzw. unverschlüsselt weitergeleitet werden können. Erlangt ein Angreifer somit einmal Zugriff auf Daten, kann er diese nach Entschlüsselung beliebig verbreiten.

Eine weitere Schwachstelle ist, dass es keine Autorisierung der Benutzer gibt. Ähnlich zu X-pire! gehen die Autoren davon aus, dass nur Personen Zugriff auf das VDO erhalten, welche auch berechtigt sind. Dies ist aber nicht immer der Fall. Eine Vanish E-Mail kann einfach weitergeleitet werden, ähnlich verhält es sich in sozialen Netzwerken, wo es üblich ist Nachrichten zu sharen. Niemand kann daher daran gehindert werden die Inhalte zu entschlüsseln, solange das Ablaufdatum nicht erreicht ist.

Generell ist die Benutzerfreundlichkeit sicher auch ein Thema, da in der derzeitigen Architektur einiges an Wissen und Können vorausgesetzt wird, um Daten durch das Vanish System sicher zur Verfügung zu stellen.

---

[227] Geambasu, Roxana, et al. "Vanish: Increasing Data Privacy with Self-Destructing Data." USENIX Security Symposium. Vol. 316. 2009.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.2.2.4 Ephemerizer

Einen etwas anderen Ansatz verwendet Ephemerizer[228]. Um Daten ein Ablaufdatum zu geben, werden diese verschlüsselt. Die Rolle des Ephemerizers ist hierbei das Erstellen, zur Verfügung stellen und zerstören der Schlüssel, die für die Verschlüsselung benötigt werden. Interessant ist, dass eine zentrale Stelle (der Ephemerizer) auch das Erstellen der unterschiedlichen Schlüssel übernimmt. Die Autoren gehen dabei davon aus, dass diese Schlüssel zwar temporär sind, aber gleichzeitig der Ephemerizer einen zentralen Schlüssel verwendet, um sich selbst zu authentifizieren und/oder alle weiteren Schlüssel davon abzuleiten. Weiters gehen die Autoren davon aus, dass auch die jeweiligen Anwender einen eigenen Langzeitschlüssel besitzen. Wichtig hierbei ist jedoch, dass der Inhalt nur mit den temporären Schlüsseln verschlüsselt werden. Durch die Ephemerizer Architektur kann dadurch sichergestellt werden, dass selbst wenn ein Angreifer unerlaubt Zugriff auf einen der Langzeit Schlüssel erlangt, Informationen, die bereits abgelaufen sind, nicht wiederhergestellt werden können.

Um ein Kopieren der Daten zu verhindern schlagen die Autoren vor, die Ephemerizer Software unter speziellen Sicherheitsmaßnahmen auf den jeweiligen Betriebssystemen laufen zu lassen, welche es nicht ermöglichen, Daten auf dem Persistenten Speicher abzulegen.

Ähnlich zu X-pire! schlagen die Autoren das Ephemerizer System vor, das Problem von Thresholding durch das Verteilen von dem Schlüssel auf einzelne Ephemerizer zu lösen, gehen aber in ihrer Definition nicht näher darauf ein.

Fazit:

Wie bereits einige Systeme zuvor, gehen die Autoren des Ephemerizer Systems davon aus, dass alle Beteiligten ein Interesse daran haben, dass Daten nicht unverschlüsselt gespeichert werden. Zusätzlich muss lokal eine Software installiert werden, die den Austausch von Schlüsseln mit dem Ephemerizer Server, sowie die Verschlüsselung selbst übernimmt.

[228] Perlman, Radia. "The ephemerizer: Making data disappear." (2005).

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

4.2.2.5 Data Revocation Service (DRS)

Data Revocation[229] Service für das Internet wurde erstmals in einem Paper 2016 vorgestellt.[230] In ihrem Verfahren konzentrieren sie sich die Autoren auf eine einfache Umsetzung Daten im Internet zu löschen. Sie gehen dabei von der Kooperation der Betreiber aus, welchen rechtlichen Regeln, wie zum Beispiel der DSGVO unterliegen. Durch diese Annahme lässt sich die technische Lösung für eine Umsetzung vereinfachen, da es nicht mehr notwendig ist komplexe Krypto Verfahren anzuwenden bzw. Benutzer keine zusätzlichen Applikationen installieren müssen, um Daten verwenden zu können.

Das DRS schränkt nicht ein, welche Daten über das System gesichert werden können. Von einzelnen gängigen Formaten wie JPEG bis zu ganzen Webseiten kann das System alle Formate abdecken.

Neben der Möglichkeit Daten löschen zu können, werden an das System fünf Hauptbedingungen gestellt, die in jedem Fall erreicht werden müssen:

- Verfügbarkeit

  Das System muss immer und überall zur Verfügung stehen, da es sonst nicht möglich ist Daten zu löschen, man akzeptiert aber, dass die Löschaktion durch den Provider nicht sofort durchgeführt werden muss.

- Skalierbarkeit

  Das System muss mit der Anzahl der zu schützenden Daten schnell und einfach skalieren können. Die Annahme ist, dass nach einer gewissen Zeit alle Daten im Internet durch ein solches System geschützt werden sollen. Dies zeigt bereits, dass es sich um riesige Datenmengen handelt, die geschützt werden müssen.

---

[229] Kieselmann, Olga. Data Revocation on the Internet. Vol. 5. Kassel university press GmbH, 2018., S 8-10

[230] Kieselmann, Olga, Nils Kopal, and Arno Wacker. "A Novel Approach to Data Revocation on the Internet." Data Privacy Management, and Security Assurance. Springer, Cham, 2015. 134-149.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Bedienerfreundlichkeit

  Einer der wichtigsten Faktoren für das System ist die Bedienerfreundlichkeit. Idealerweise sollte die Verwendung für Benutzer, die Inhalte im Internet ansehen, transparent sein. Der Aufwand, neue Inhalt über das System zu schützen, sollten so gering wie möglich sein.

- Keine Zensur

  Es soll keine Möglichkeit für private oder öffentliche Stellen geben, das System zu zensurieren. Dies bedeutet, dass nur der Eigentümer bzw. jene Person, die die Daten veröffentlicht hat, diese auch löschen kann.

- Privatsphäre

  Die Privatsphäre und Anonymität der Benutzer müssen auch durch dieses System gegeben sein. Im Speziellen darf es zu keinem Zeitpunkt möglich sein, die Identität eines Anwenders herauszufinden.

Basierend auf diesen Bedingungen funktioniert das DRS System wie folgt:

Jedem Objekt, das veröffentlicht werden soll, muss zuerst ein eindeutiger Schlüssel zugewiesen werden. Hierfür gibt es mehrere Methoden. DRS bevorzugt die Verwendung einer Hash Funktion. Der Vorteil dabei ist, dass jederzeit aus dem Objekt selbst der Schlüssel generiert werden kann. In einigen Fällen kann es notwendig sein, dass geänderte Dateien den gleichen Schlüssel erhalten. Dies würde durch eine Standard Hash Funktion nicht erreicht werden, da jede kleine Änderung des Inhaltes sofort zu einem anderen Schlüssel führen würde. In diesem speziellen Fall schlägt man vor, eine Robuste Hash[231] Funktion zu verwenden, um alle Derivate eines Bildes mit dem gleichen Schlüssel zu versehen.

[231] Venkatesan, Ramarathnam, et al. "Robust image hashing." Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101). Vol. 3. IEEE, (2000): 664 -666

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Dieser Schlüssel muss nun eindeutig mit dem Objekt verbunden werden. Am einfachsten wird dies durch das Einfügen des Schlüssels in den Metainformationen des Objektes erreicht. Dies ist notwendig, damit das System erkennt, welche Daten geschützt sind.

Der nächste Schritt ist, dass der Eigentümer das Objekt in dem DRS publiziert. Um die Daten sicher und skalierbar abzulegen, schlägt das DRS System vor, einen DHT[232] (siehe auch 4.2.2.3) auf Basis eines P2P Netzwerkes (z.B.: Chord[233] oder Kademlia[234]) zu realisieren. In diesen DHTs wir der generierte Schlüssel des Objektes als Key und der Status („active“ oder „“revoked“) als Value abgelegt.

Damit das System sicherstellt, dass nur die Eigentümer der Objekte deren Status auch verändern können, ist es notwendig den jeweiligen Benutzer zu authentifizieren. Um nicht auf Passwörter oder Zertifikate angewiesen zu sein, setzt das DRS System ein Feige-Fiat-Shamir Protocol ein.[235] Dieses Protokoll basiert darauf, dass in der ersten Phase eine zufällige Nummer generiert wird, welcher in der zweiten Phase der Authentifizierung für die Überprüfung der Identität verwendet wird. Bei der generierten Nummer handelt es sich um den Schlüssel S‘. Während der Authentifizierung werden den Anwendern unterschiedliche Aufgaben gestellt, für deren Lösung der Schlüssel verwendet werden muss. Die Verwendung des Feige-Fiat-Shamir Protokolls ermöglich es, die häufigere Operation der Registrierung sehr einfach zu gewährleisten, wobei das Update des Status aufwendiger ist. Da man aber davon ausgehen kann, dass mehr Objekte registriert, als gelöscht werden, ist dies für die Ersteller des DRS vertretbar.

---

[232] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

[233] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

[234] Maymounkov, Petar, and David Mazieres. "Kademlia: A peer-to-peer information system based on the xor metric." International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002.

[235] Feige, Uriel, Amos Fiat, and Adi Shamir. "Zero-knowledge proofs of identity." Journal of cryptology 1.2 (1988): 77-94.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Für alle geschützten Objekte ist es nun notwendig, dass der Service-Provider bei jeder Anfrage überprüft, ob dieses noch aktiv ist. Eine genaue Darstellung des Protokollablaufs liefert die Abbildung 12: DRS Protokoll Übersicht.

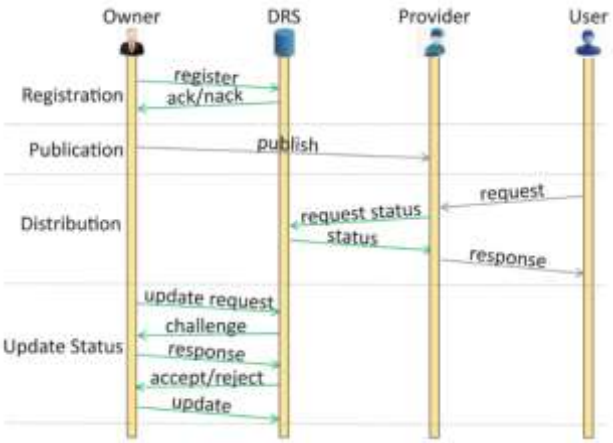

Abbildung 12: DRS Protokoll Übersicht[236]

Fazit:

Das DRS bietet eine einfach und sehr skalierbare Möglichkeit Daten vor dem unerlaubten Zugriff zu schützen bzw. diese als gelöscht zu markieren. Das System kann transparent in bestehende Infrastrukturen integriert werden und verhindert damit größere Probleme in der Implementierung.

Die größte Schwachstelle ist jedoch, dass man davon ausgeht, dass die Provider durch einen rechtlichen Rahmen dazu angehalten werden, ein solches System auch einzusetzen und nicht gegen die „Regeln“ zu verstoßen. Technologisch und architekturell sind keine Vorgehensweisen getroffen worden, sollte dies nicht der Fall sein. Eine weitere Schwachstelle ist, dass das System nur auf Provider abzielt. Jede Person, die ein Objekt einmal von diesem ausgeliefert bekommen hat, kann dieses jederzeit kopieren und ungehindert verbreiten. Selbst wenn das Objekt dem gleichen Provider wieder übergeben wird. Solange der Key in den

[236] Kieselmann, Olga, Nils Kopal, and Arno Wacker. "A Novel Approach to Data Revocation on the Internet." Data Privacy Management, and Security Assurance. Springer, Cham, 2015. 134-149.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Metainformationen entfernt wird, hat der Provider keine Möglichkeit festzustellen, dass es sich dabei um das gleiche Objekt handelt.

4.2.2.6 Secure Overlay Cloud Storage (FADE)

Bei FADE[237], welches erstmals in einem Paper 2012 vorgestellt wurde und einige der zuvor beschriebenen Technologien verbindet, handelt es sich um eine sichere Cloud-Abstraktion, die es ermöglicht Daten mit Richtlinien zu versehen. Diese Policies können unterschiedliche Ausprägungen haben (z.B. Verfallsdatum, Lese- und Schreiberecht für gewisse Benutzer, …). Zusätzlich bietet FADE eine generalisierte Möglichkeit, Dateien zeitlich zu löschen (siehe Kapitel 4.2.2.3).

Um dies gewährleisten zu können, weist FADE jeder Datei eine atomare Zugriff Policy zu. Diese kann aus mehreren atomaren Policies bestehen. Jede davon wertet ein spezielles Kriterium aus und entscheidet, ob der Benutzer zu diesem Zeitpunkt, mit den jeweiligen Client auf die Datei zugreifen darf oder nicht.

Diese Art der Zugriffskontrolle ermöglicht nicht nur das „Löschen" von Daten auf Basis eines Verfallsdatums, sondern ermöglicht viele unterschiedliche Szenarien;

- Löschen von Daten, wenn eine Person das Unternehmen verlässt,
- Zugriffserlaubnis auf Basis des Clients, der auf die Dateien zugreift.

Um dies sicherstellen zu können, weist FADE jeder Policy einen Kontrollschlüssel (reference to symetric key) zu. Diese Schlüssel werden in einem Schlüssel Management System[238] verwaltet. Ähnlich zu dem Vanish System wird jede Datei mit einem Datenschlüssel gesichert. Dieser Schlüssel wird wiederum mit einem Kontrollschlüssel der jeweiligen Policy verschlüsselt. Wenn sich der Besitzer der Datei dazu entschließt, die Policy zu invalideren, wird der Schlüssel aus dem Key Management System gelöscht. In diesem Fall kann der Schlüssel nicht wiederhergestellt werden und dadurch die gesicherte Datei nicht wieder entschlüsselt werden. FADE geht nun davon aus, dass die Datei sicher gelöscht ist und würde in weiterer Folge alle Dateien, von denen die Policy invalidiert

[237] Begum, Gousiya, and M. Shravya. "Secure Cloud Storage with File Assured Deletion."
[238] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

wurde, auch löschen. Sollte dies der Cloud-Provider nicht sofort durchführen, bzw. Sicherungen der Daten haben, können diese durch den nichtexistierenden Schlüssel nicht mehr gelesen werden.

FADE besteht aus zwei Komponenten, die zusammenarbeiten müssen:

- FADE Client

  Dieser Client bildet das Interface zwischen Datenprovider bzw. Empfänger (lokales Filesystem, Webbrowser) und der Cloud. Er ist für die Ver- und Entschlüsselung der Daten verantwortlich und transferiert die Daten von bzw. aus der Cloud. Der Client kommuniziert auch mit dem Key Manager, um die notwendigen Schlüsseloperationen durchzuführen.

- Key Manager

  Die Aufgabe des Key Managers ist die sichere Aufbewahrung und Löschung der Schlüssel, die für die Policy verwendet werden. FADE in der initialen Version[239] basiert auf einem Quorum von Key Managern, wobei jeder Manager als einzelne Identität gesehen werden kann.

Für die Installation stehen unterschiedliche Varianten zur Verfügung. In ihrem ursprünglichen Paper beschrieben Yang Tang und Patrick P.C Lee eine lokale Installation. In diesem Fall wird der Client auf der jeweiligen Maschine, auf der die Daten geschrieben und gelesen werden sollen, installiert. Ebenso ist auch eine zentrale Installation möglich, in der die Daten in Transit mittels der üblichen Sicherheitstechniken (TLS/SSL)[240] gesichert werden.

Bei dem Design von FADE wurden zwei Sicherheitsziele betrachtet, die für die Sicherheit von Daten in der Cloud wichtig sind:

---

[239] Tang, Yang, et al. "Secure overlay cloud storage with access control and assured deletion." IEEE Transactions on dependable and secure computing 9.6 (2012): 903-916.
[240] Dierks, Tim, and Eric Rescorla. "The transport layer security (TLS) protocol version 1.2." (2008): 5246.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

- Policy basierter Zugriff

  Der FADE Client darf nur auf Daten zugreifen, die aktive Policies haben die vom Client überprüft wurden.

- Policy basiertes Löschen

  Sobald eine Policy nicht mehr gültig ist, müssen die Daten gelöscht werden.

Um dies sicherstellen zu können, müssen gewisse Voraussetzungen gegeben sein:

- Jeder FADE Client darf keine Kopie des Data Keys, welcher für die Verschlüsselung von Daten verwendet wird, lokal speichern.

- Die Daten dürfen lokal nicht entschlüsselt gespeichert werden.

- Nur die verschlüsselte Version des Data Keys und der Daten werden in der Cloud gespeichert.

Fazit:

Die oben angeführten Voraussetzungen zeigen bereits die Schwachstellen von FADE. Speziell bei lokalen Installationen kann im Internet nicht davon ausgegangen werden, dass der Client nicht verändert oder der Data Key sowie die entschlüsselten Daten lokal gespeichert werden. Bei einer Anwendung von FADE innerhalb eines Unternehmens, kann dieses bis zu einem gewissen Grad sicherstellen, dass nur ein spezieller Client verwendet wird. Auch hier kann es bei lokalen Client-Installationen leicht zu Angriffen kommen. Bei einem zentralen Deployment kann zwar das Risiko eines Angriffes auf den Client verhindert werden, es stellt sich aber die Frage, wo ein solches passieren könnte um die Vorteile der Cloud (Skalierbarkeit, Erreichbarkeit) nicht zu negieren. Ein Deployment in der Cloud ist durch die lokale Verwaltung der Schlüssel nicht ratsam, da sonst der Cloud-Provider wieder Zugriff auf die Daten erreichen könnte. Eine Installation bei einem anderen Cloud-Provider bzw. einem lokalen Hoster könnte das Risiko minimieren.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Gousiya Begum[241] beschreibt in einer erweiterten Version die Verwendung von „blinded RSA“, welche eine gravierende Schwachstelle von FADE beheben würde. In diesem Fall wird der Data Key nicht direkt mit dem Client geteilt, sondern das RSA Modul ist für die Ver- und Entschlüsselung verantwortlich. Dadurch kann der Client diesen nicht speichern oder ein Angreifer die Daten in der Kommunikation abgreifen. Hier stellt sich die Frage, wo dieses Service installiert wird. Sämtliche großen Cloud-Provider bieten heute ähnliche Dienste an. Diese werden speziell zertifiziert, trotzdem sind die Daten in der Cloud gespeichert.

Ein weiterer Nachteil von FADE ist, dass es ein Overlay auf basierenden Technologien darstellt, welche bereits sehr gut in unterschiedliche Systeme integriert sind. Weiters wird die Verarbeitung von Daten in der Cloud - welche durch sehr gute Integration und Tools von den Cloud-Providern immer einfacher wird - komplett ausgeklammert.

4.2.2.7 Digitales Wasserzeichen

Wie bereits in dem Kapitel 4.2.1 Technische Herausforderungen erwähnt, besteht die Herausforderung nicht nur darin, Daten zu löschen, sondern auch festzustellen, wer die Eigentümer von diesen ist. Hierfür gibt es Methoden, die dies auch nach unerlaubtem Kopieren von Daten ermöglichen.

Im Buch “Digital Watermarking and Steganography” von Ingemar Cox, Matthew Miller und Jeffrey Bloom wird die Anwendung von Wasserzeichen wird wie folgt definiert:

> *“We define watermarking as the practice of impeccability altering a Work to embed a message about the work”*[242]

Auch wenn der Hauptfokus von Wasserzeichen ursprünglich auf Bildern, Text und Video lag, gibt es Möglichkeiten andere Inhalte mit einem digitalen Wasserzeichen zu versehen (z.B: binäre Bilder oder Texte). [243]

---

[241] Begum, Gousiya, and M. Shravya. "Secure Cloud Storage with File Assured Deletion."
[242] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan Kaufmann, (2007): 2
[243] Begum, Gousiya, and M. Shravya. "Secure Cloud Storage with File Assured Deletion."

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Es gibt einige Vorteile von Wasserzeichen gegenüber anderen Techniken wie dem Abspeichern von Meta-Informationen in den Dateien:

- Sie sind unmerklich

  Das bedeutet, dass sie nicht mit freiem Auge festgestellt werden können und beeinträchtigen damit nicht die Ästhetik eines Werkes (z.B. Bild, Text, Video).

- Sie sind untrennbar mit dem Originalwerk verbunden

  Sie können vom Originalwerk nicht entfernt werden, wenn sie einmal eingefügt wurden.

- Sie unterliegen denselben Transformationen wie das Originalwerk

  Auch wenn die Daten analog weiterverbreitet (z.B. ausgedruckt) werden, muss das Wasserzeichen robust genug sein, einer durch den Kanal verursachten Verschlechterung standzuhalten und nach der Transformation trotzdem dem Original zugeordnet zu werden.

Grob gesprochen gibt es vier Komponenten, die bei der Verwendung eines digitalen Wasserzeichens relevant sind:

- Original (Cover Work)

  Jener Inhalt der mit einem Wasserzeichen versehen werden soll.

- Payload

  Der Inhalt des digitalen Wasserzeichens, welcher in die ursprüngliche Arbeit eingebettet werden soll.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Embedder

Der Embedder ist jene Komponente, die das Original und den Payload als Eingabe übernimmt und daraus ein neues Objekt generiert. Hierbei gibt es unterschiedliche Methoden, abhängig von den jeweiligen Originalformat. Wichtig ist, dass die mit einem Wasserzeichen versehenen Daten über das gleiche Format, wie das Original, verfügen.

- Detector

Der Detector wird verwendet, um sicherzustellen, ob Daten von dem Original abstammen. Wenn das Original vorhanden ist, kann der Detector dieses verwenden und mit dem Objekt vergleichen (non-blind watermarking). Sollte das Original nicht vorhanden sein, versucht der Detector die Stärke des Payload Signales (blind watermakring) zu verifizieren[244].

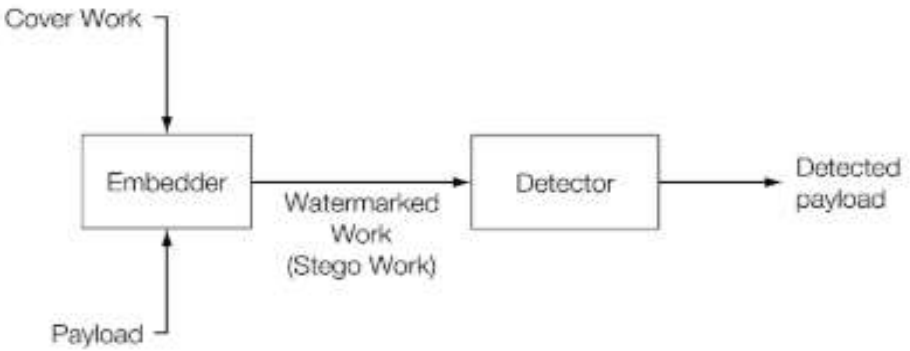

Abbildung 13: Prozess zur Überprüfung von digitalen Wasserzeichen[245]

[244] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. IEEE, 2005.

[245] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. IEEE, 2005.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Fazit:

Speziell in einem Umfeld, wo nicht gewährleistet werden kann, dass Daten nicht analog weiterverarbeitet werden, bieten Wasserzeichen eine gute Möglichkeit sicherzustellen, dass sie von einem Original stammen. Dies kann erfolgen, ohne die Ästhetik des Originales zu verändern oder dass es der Anwender es feststellen kann.

4.2.2.8 Digital Rights Management (DRM)

Digital Rights Management Systeme werden verwendet um die Verbreitung und Verwendung von wertvollen Inhalten (z.B. Filme) zu kontrollieren. Hierzu ist es notwendig, dass diese einen permanenten und sicheren Schutz bieten. Ein DRM-System sollte eine flexible und einfache Möglichkeit bieten, die unterschiedlichen Formate und Inhalte (Film, Bild, Buch, Video Stream, …) auf unterschiedlichen Plattformen (z.B. PC, Mobiltelefon, Tablets, …) zu unterstützten[246].

Um dies zu erfüllen bedient sich ein DRM-System einer digitalen Lizenz, welche Benutzern unterschiedliche Rechte zusichert. Diese können zentral verwaltet werden und sehr generisch auf die Bedürfnisse des Eigentümers bzw. Verteilers zugeschnitten sein. Es ist möglich, die Anzahl der Aufrufer, die Dauer der Abrufzeit sowie die Anzahl der Geräte, auf denen der Inhalt angesehen werden kann, zu beschränken.

Ein typisches DRM-System besteht normalerweise aus vier Teilnehmern und den folgenden Prozessen:

[246] Liu, Qiong, Reihaneh Safavi-Naini, and Nicholas Paul Sheppard. "Digital rights management for content distribution." Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. (2003): 49-58

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

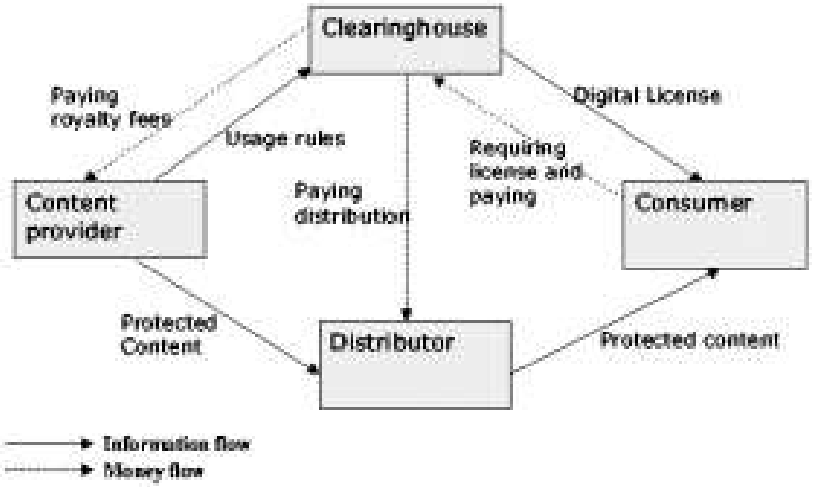

Abbildung 14: DRM-System - Prozessübersicht[247]

- Content-Provider

Eine Peron oder eine Organisation, die die Rechte an den Inhalten, die geteilt werden sollen, halten.

- Verteiler

Jene Person oder Organisation, die einen Verteilkanal für die Inhalte anbieten möchte. Dies kann eine Webseite, ein Online-Shop oder ein Einzelhändler sein.

- Konsument

Der Anwender des Verteilkanals, über den er Inhalte beziehen möchte. Diese Inhalte können entweder gestreamt, heruntergeladen oder über ein digitales Medium bezogen werden.

[247] Liu, Qiong, Reihaneh Safavi-Naini, and Nicholas Paul Sheppard. "Digital rights management for content distribution." Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. (2003): 49-58

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

- Verrechnungsstelle

  Ist damit beauftragt die Bezahlung für die Benützung der Inhalte abzuwickeln. Sie nimmt von dem Konsumenten die Benützungsgebühr entgegen und zahlt an den Content-Provider die Lizenzgebühren sowie an den Verteiler die Verteilgebühr anhand eines zuvor festgestellten Aufteilungsschlüssels. Zusätzlich speichert und überwacht sie die Lizenzverwendung der unterschiedlichen Konsumenten. Nicht jede Verwendung von Inhalten muss zwangsweise kostenpflichtig sein.

Typischerweise stellt der Content-Provider im ersten Schritt einen digitalen Inhalt dem Verteiler zur Verfügung. Wichtig hierbei ist, dass es keinen einheitlichen Standard für DRM-Systeme gibt. Der digitale Inhalt wird verschlüsselt und für den jeweiligen Verteilerkanal aufbereitet. Einige Content-Provider verwenden hierfür auch Watermarking Methoden (siehe 4.2.2.7), um zu gewährleisten, dass es sich um ihren Inhalt handelt.

Als nächstes wird der geschützte Inhalt an den Verteiler weitergegeben, welcher ihn auf seinem Verteilerkanal (typischerweise Web-Server) zum Bezug anbietet. Danach wird die Lizenz für den Inhalt an die jeweilige Verrechnungsstelle gesendet. Diese regelt, welche Benutzungsregeln für den Inhalt zutreffen (z.B. Kosten für pay-per-view oder one-week-rental sowie Weiterverbreitungsrechte).

Wenn sich ein Kunde dazu entscheidet, den Inhalt zu benützen, bezieht er diesen von dem Verteilerkanal. Um den Inhalt auch wirklich ansehen zu können, muss er dafür eine gültige Lizenz von der Verrechnungsstelle besitzen.

Da es keinen einheitlichen Standard für den Schutz von Inhalten und den Aufbau von DRM-Systemen gibt, behelfen sich die meisten Anbieter mit sogenannten Plug-ins. Hierbei werden Betrachtungsprogramme, die nicht mit DRM-Systemen umgehen können (z.B. Windows Media Player) mittels Software erweitert, so dass sie die Einhaltung der Lizenz erzwingen. Da diese Programme den unverschlüsselten Inhalt durch die Plug-ins übergeben bekommen, ist es wichtig, dass die Plugin-Struktur sicher ist, sonst Inhalte abgegriffen werden können.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Einen interessanten Punkt beleuchtet das Paper Privacy-Preserving DRM[248] hinsichtlich der Möglichkeit anonym an einem DRM-System teilzunehmen. Der primäre Fokus in diesem Dokument ist, wie in einem DRM-System anonym bezahlt werden kann. Wenn in einem verbunden Netzwerk Inhalte mittels Digital Rights Management[249] geschützt werden und darüber auch das Löschen von Daten sichergestellt werden kann, bleibt die Frage der möglichen anonymen Nutzung unbeantwortet, da alle Benutzer im System autorisiert sein müssen.

Fazit:

DRM-Systeme sind seit vielen Jahren ein erfolgreiches Mittel um Inhalte vor der unberechtigten Verbreitung oder Verwendung zu schützten. Trotzdem sind sie in den meisten Bereichen Nischenanwendungen geblieben und haben sich kaum zu einem einheitlichen Standard entwickelt. Besonders die Film- und Musikindustrie verwenden heute in den meisten Bereichen DRM geschützte Inhalte. Die größte Herausforderung und auch Schwachstelle von DRM-Systemen liegt in den notwendigen Plug-ins, welche meistens nur auf einige wenige File-Formate anwendbar sind. Für geschlossene Netzwerke bieten sie einen guten Schutz, die Ausweitung auf eine größere Kunden- und Inhaltsbasis ist aber fraglich, da auch die Systemarchitekturen nicht für die Verteilung ausgelegt sind.

4.2.2.9 User basiertes semantisches Rechtemodel zur Validierung von Inhalten

Heutige DRM-Systeme sind nicht auf die neuen Anforderungen von Social Media-Plattformen ausgerichtet. In einem neuen Ansatz[250] wird hier versucht, existierende DRM-Systeme auf die Anforderungen einer „share and distribute“ Gesellschaft zu erweitern. Hierfür wird vorgeschlagen, die „Rights Expression Specification“, welche in den meisten DRM-Systeme auf eine strikte Restriktion

[248] Perlman, Radia. "The ephemerizer: Making data disappear." (2005).
[249] Closa, Daniel. Patent Law for Computer Scientists. Ed. Jo Falk Giemsa. Springer Berlin Heidelberg, (2010): 63ff
[250] Kim, Jeongmin, et al. "Design of user-centric semantic rights model for validation of user-generated content." *Cluster Computing* 19.3 (2016): 1261-1273.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

von der Benützung der Inhalte abzielt, auf eine mehr kundenorientierte use, share und distribute auszuweiten.[251]

In ihrem MPEG–21 Standard der Movie Pictures Expert Group (MPEG), wird vorgeschlagen, eine Rights Expression Langue (REL) sowie ein Rights Data Dictionary (RDD) zu bilden.[252]

REL definiert hierbei Rechte, die eine Person auf einer gewissen Ressource ausführen darf (z.B. drucken, abspielen, löschen). Dieses Modell ist an sich erweiterbar, geht aber von einem zentralen Content-Provider (IssuABer) aus. In den sozialen Netzwerken, wo Daten durch mehrere Personen weiterverteilt werden können, ist dies nicht ausreichend.

Aus diesem Grund definieren die Autoren ein neues Model auf Basis von Actor Model (User), Ressource Model (Content) und einem License Model wie in Abbildung 14 gezeigt.

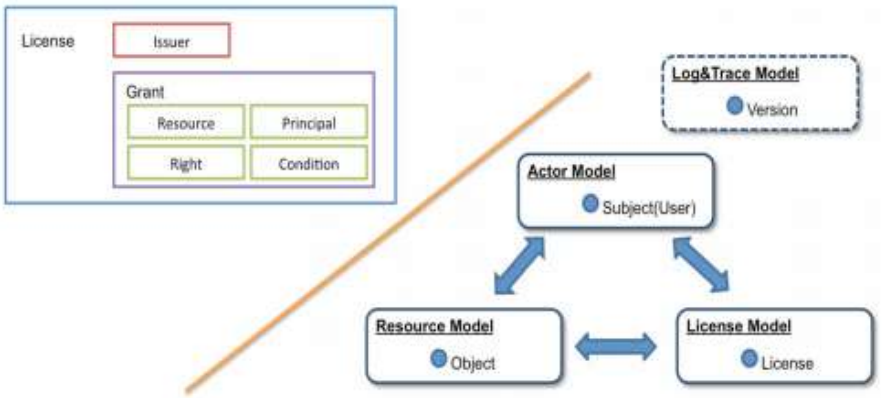

Abbildung 15: Actor Modell [253]

[251] Rosenblatt, Bill, Bill Trippe, and Stephen Mooney. "Digital Rights Management." New York (2002).

[252] Wang, Xin, et al. "The MPEG-21 rights expression language and rights data dictionary." IEEE Transactions on Multimedia 7.3 (2005): 408-417.

[253] Wang, Xin, et al. "The MPEG-21 rights expression language and rights data dictionary." IEEE Transactions on Multimedia 7.3 (2005): 408-417.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Auch die System-Architektur wird von den Autoren auf ein verteiltes Service[254] umgestellt wie Abbildung 16: System zeigt.

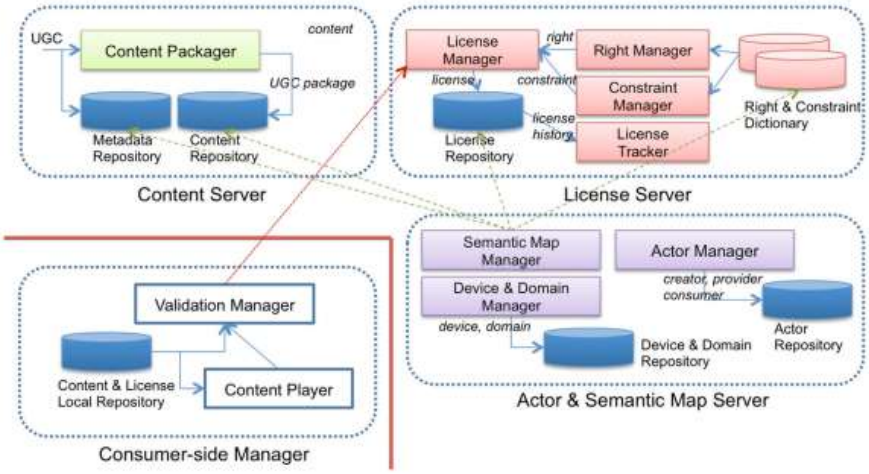

Abbildung 16: System Architektur[255]

In dieser Architektur ist der Content Server dafür verantwortlich, User generierte Inhalte zu annotieren und zu verparken. Diese Inhalte können danach in dem Content Repository gespeichert werden. Nachdem der Benutzer die Inhalte hochgeladen hat, besteht die Möglichkeit mehrere unterschiedliche Lizenzen auf dem Lizenzserver zu generieren. Dieser hat die Möglichkeit, Lizenzen, Rechte und Bedingungen zu verwalten. Der Benutzer generiert hierfür ein oder mehrere Rechte (z.B. ansehen, drucken) und die dazugehörigen Bedingungen. Ein Beispiel wäre, dass nur jene Benutzer den Inhalt drucken dürfen, die bereits ein Objekt geshared haben. Danach können, basierend auf den Rechten und Bedingungen, mehrere Lizenzen generiert werden.

---

[254] Canali, Claudia, Michele Colajanni, and Riccardo Lancellotti. "A Two-level distributed architecture for the support of content adaptation and delivery services." Cluster Computing 13.1 (2010): 1-17.

[255] Canali, Claudia, Michele Colajanni, and Riccardo Lancellotti. "A Two-level distributed architecture for the support of content adaptation and delivery services." Cluster Computing 13.1 (2010): 1-17.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Fazit:

Das vorgestellte Modell bietet eine neue Möglichkeit DRM-Systeme auf die neuen Anforderungen im Social Media-Umfeld zu erweitern. Leider bleibt das Team eine technische Evaluierung ihres Modells schuldig. Besonders interessant hierfür wäre, wie dieses System in existierende Social Media-Services integriert werden könnte. DRM-Systeme lösen dieses Problem durch Erweiterung existierender Betrachtungsprogramme mittels Plug-in-Technologien. Diese Möglichkeit ist in heutigen Social Media-Plattformen jedoch nicht so einfach gegeben. Wo in Browsern noch Plug-in Möglichkeiten bestehen, ist es derzeit nicht vorstellbar, wie diese Methoden ohne die Zustimmung der Social Media-Plattformen in mobile Applikationen eingebaut werden könnten.

4.3 Fazit und Lösungsansätze

Generell ist festzuhalten, dass das Löschen von Daten in einem sehr verteilten und nicht zentral organisierten System wie dem Internet eine sehr komplexe und schwierig zu adressierender Herausforderung ist.

Rechtlich hat die Europäische Union mit dem DSGVO einen sehr wichtigen Schritt getätigt, um personenbezogen Daten aus dem Internet zu löschen. Da die meisten Unternehmen in der Europäischen Union ihre Services anbieten, ist sie natürlich nicht nur auf die Unternehmen in Europa beschränkt und hat schon heute einen wichtigen Beitrag geleistet, weltweit das Löschen von Daten zu ermöglichen. Hier ist jedoch festzuhalten, dass selbst die DSGVO sich nur auf einen Teil von Daten beschränkt. Die meisten technischen Lösungsvorschläge basieren entweder auf dem Prinzip Daten zu verstecken oder zu verschlüsseln. Beide Methoden besitzen Schwachstellen, welche noch nicht ausreichend adressiert wurden. Das Verstecken der Daten ist auf die Kooperation der Unternehmen angewiesen und verschiebt den Fokus damit von einer technisch sicheren Lösung auf das Rechtssystem. Verschlüsselungsmethoden versuchen alle Eventualitäten technisch abzubilden und sind damit technisch anspruchsvoll. Keines der vorgestellten Systeme wurde mit der riesigen Anzahl an Daten im Internet getestet. Es ist unwahrscheinlich, dass sie ausreichend skalieren, um die derzeit im Umlauf befindlichen Daten zu adressieren. Dazu führen sie noch zu

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

einem Bruch mit allen derzeit verwendeten Tools, welcher in der heuteigen Zeit kaum umsetzbar erscheint.

Um ein generelles Löschen von Daten im Internet zu gewährleisten, wird es notwendig sein technische sowie rechtliche Aspekte miteinander zu verbinden.

4.3.1 Mögliche rechtliche Ansätze

Die größte Herausforderung bezüglich der rechtlichen Rahmenbedingungen ist, dass das Internet aufgrund seiner Globalität in die Zuständigkeit unterschiedlicher Rechtssysteme fällt. Es gibt hierfür keine Möglichkeit ein zentrales bzw. weltweit gültiges Recht auf das Löschen von Daten umzusetzen. Natürlich haben Rechtssysteme von großen Wirtschaftsräumen wie die Europäische Union oder Amerika die Möglichkeit, neue Regeln auch in anderen Regionen anzutreiben. Ein globales Abkommen bezüglich des Rechts auf das Löschen von Daten gibt es jedoch nicht. Um dies verwirklichen, gäbe Ansätze wie bilaterale Abkommen oder internationale Verträge.

Idealerweise könnte man auch in Zeiten der Digitalisierung und Automatisierung die bestehenden Bestrebungen rund um die Menschenrechtserklärung auf ein Recht auf Privatsphäre und Datenschutz als Menschenrecht verstärken. In diesen wäre es möglich ein Recht auf Löschung von privaten Daten zu verankern. Hier wäre natürlich, wie auch in der DSGVO, eine Abwägung des öffentlichen Interesses durchzuführen damit eine Zensur von Informationen unterbunden wird. So lange es eine solche Vereinbarung nicht getroffen werden kann, wäre es sinnvoll bilaterale Abkommen, wie das Privacy Shield Abkommen mit der USA auf neue Beine zu stellen.

4.3.2 Mögliche technische Ansätze

Grob gesprochen gibt es zwei große Herausforderungen, die adressiert werden müssen, um das Recht auf Löschen umzusetzen:

- Authentifizierung und Autorisierung für die Löschung, sowie
- das Auffinden und Löschen von Kopien.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Nachdem das Löschen auf fremden Computern so gut wie unmöglich sichergestellt werden kann (Hostile Host Problem) wird es notwendig sein folgende technischen Herausforderungen zu schaffen:

- Meldesystem für Löschung von Daten

  Wie im Kapitel 4.2.2.5 beschrieben, sollte es eine zentrale Möglichkeit geben, Provider über den Wunsch zu informieren, dass Daten gelöscht werden sollen. Hierfür wäre es von Vorteil, wenn es ein zentrales Meldesystem (ähnlich dem DNS-System) geben würde, in welchem die Anfragen gespeichert und nachvollzogen werden können. Durch die große Anzahl an zu erwartenden Anfragen, müsste das System verteilt und so weit als möglich durch APIs automatisiert verwaltbar sein.

- Sicherheit als Teil des Datenformates

  Es wäre sinnvoll in Zukunft bereits bei dem Design von Datenformaten die Möglichkeit des Löschens zu berücksichtigen. Hierfür könnte ein Containerformat entwickelt werden, in welchem die unterschiedlichen Dateiformate integriert werden.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 5
Quellenverzeichnis

5.1 Literatur

[1] Aggarwal, Charu C. "Data classification." Data Mining. Springer, Cham, 2015

[2] ARM. “Security technology building a secure system using trustzone technology” (2006)

[3] Backes, Julian, et al. "X-pire!-a digital expiration date for images in social networks." arXiv preprint arXiv:1112.2649 (2011).

[4] Backes, Michael, et al. "X-pire 2.0: a user-controlled expiration date and copy protection mechanism." Proceedings of the 29th annual ACM Symposium on applied computing. (2014): 1633--1640

[5] Balaban, D, “Understanding CAPTCHA-solving services in an economic context” (2011): 3: evaluation of the human-based services

[6] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolf. „Brief History of the Internet.“ Internet Society, (1997)

[7] Becker, Jack, and Elana Bailey. "A comparison of IT governance & control frameworks in cloud computing." (2014)

[8] Becker, Steffen, Gunnar Brataas, and Sebastian Lehrig, eds. “Engineering Scalable, Elastic, and Cost-Efficient Cloud Computing Applications: The CloudScale Method. Springer, (2017)

[9] Begum, Gousiya, and M. Shravya. "Secure Cloud Storage with File Assured Deletion."

[10] Balachander Krishnamurthy and Craig E. Wills. "On the leakage of personally identifiable information via online social networks.", Association for Computing Machinery, (2009):7

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[11] Bergauer/Jahnel/Mader/Staudegger (Hrsg). „jusIT Spezial: DSGVO.“ LexisNexis (2018)

[12] Bernstein, David. "Containers and cloud: From lxc to docker to kubernetes." IEEE Cloud Computing 1.3 (2014)

[13] Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl. „DSG.“ Linde (2018)

[14] Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. Cloud computing: Principles and paradigms. Vol. 87. John Wiley & Sons, (2010)

[15] Canali, Claudia, Michele Colajanni, and Riccardo Lancellotti. "A Two-level distributed architecture for the support of content adaptation and delivery services." Cluster Computing 13.1 (2010): 1-17.

[16] Celesti, Antonio, et al. "Three-phase cross-cloud federation model: The cloud sso authentication." 2010 Second International Conference on Advances in Future Internet. IEEE, 2010.

[17] Chew, Monica, and J. Doug Tygar. "Image recognition captchas." International Conference on Information Security. Springer, Berlin, Heidelberg, (2004) 268--279

[18] Cholez, Thibault, et al. "Detection and mitigation of localized attacks in a widely deployed P2P network." Peer-to-Peer Networking and Applications 6.2 (2013): 155-174.

[19] Closa, Daniel. Patent Law for Computer Scientists. Ed. Jo Falk Giemsa. Springer Berlin Heidelberg, (2010): 63ff

[20] Coulouris, George F., Jean Dollimore, and Tim Kindberg. Distributed systems: concepts and design. pearson education, 2005.

[21] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan kaufmann, (2007):

[22] Dierks, Tim, and Eric Rescorla. "The transport layer security (TLS) protocol version 1.2." (2008): 5246.

[23] Douceur, John R. "The sybil attack." International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002.

[24] Falkner, Jarret, et al. "Profiling a million user DHT." Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. 2007.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

[25] Feige, Uriel, Amos Fiat, and Adi Shamir. "Zero-knowledge proofs of identity." Journal of cryptology 1.2 (1988): 77-94.

[26] Fielding, Roy Thomas, Architectural Styles and the Design of Network-based Software Architectures, Dissertation University of California, (2000)

[27] Geambasu, Roxana, et al. "Vanish: Increasing Data Privacy with Self-Destructing Data." USENIX Security Symposium. Vol. 316. (2009)

[28] Gerrit Hornung/ Kai Hoffmann. „Ein »Recht auf Vergessenwerden«? Anspruch und Wirklichkeit eines neuen Datenschutzrechts“, JZ 68 (2013)

[29] Gutmann, Peter. "Secure deletion of data from magnetic and solid-state memory." Proceedings of the Sixth USENIX Security Symposium, San Jose, CA. Vol. 14. (1996) 77—89

[30] Hannes, Federrath, Karl-Peter Fuchs, Dominik Herrmann, Daniel Maier, Florian Scheuer, und Kai Wagner. „Grenzen des digitalen Radiergummis.“ Datenschutz und Datensicherheit - DuD 35 (2011): 403-407

[31] Herbst, Nikolas Roman, Samuel Kounev, and Ralf Reussner. "Elasticity in cloud computing: What it is, and what it is not." 10th International Conference on Autonomic Computing ({ICAC} 13). (2013).

[32] Ilya Grigorik, High Performance Browser Networking, O'Reilly Media, (2013):

[33] Jürgen Kühling, Manuel Klar, Florian Sackmann, "Datenschutzrecht." 4. Auflage. Heidelberg 2018, ISBN 978-3-8114-4571-0

[34] Kieselmann, Olga. Data Revocation on the Internet. Vol. 5. kassel university press GmbH, 2018., S 8-10

[35] Kieselmann, Olga, Nils Kopal, and Arno Wacker. "A Novel Approach to Data Revocation on the Internet." Data Privacy Management, and Security Assurance. Springer, Cham, 2015. 134-149.

[36] Kim, Jeongmin, et al. "Design of user-centric semantic rights model for validation of user-generated content." Cluster Computing 19.3 (2016): 1261-1273

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[37] Kohl, John T. "The use of encryption in Kerberos for network authentication." Conference on the Theory and Application of Cryptology. Springer, New York, NY, (1989): 35–43.

[38] Liu, Qiong, Reihaneh Safavi-Naini, and Nicholas Paul Sheppard. "Digital rights management for content distribution." Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. (2003): 49-58

[39] Lukas Feiler/Bernhard Horn. „Umsetzung der DSGVO in der Praxis.“ Verlag Österreich (2018)

[40] Maymounkov, Petar, and David Mazieres. "Kademlia: A peer-to-peer information system based on the xor metric." International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002.

[41] Michael Rohrlich. „Cloud Computing - Rechtliche Grundlagen.“ Rechtliche Grundlagen, entwickler.press 2014

[42] Melzer, Ingo. Service-Orientierte Architekturen Mit Web Services. Heidelberg: Spektrum Akademischer Verlag GmbH, (2010)

[43] Nolte, Norbert. “Zum Recht Auf Vergessen Im Internet: Von Digitalen Radiergummis Und Anderen Instrumenten.” Zeitschrift Für Rechtspolitik, vol. 44, no. 8, (2011)

[44] Perlman, Radia. "The ephemerizer: Making data disappear." (2005).

[45] Preston Gralla, and Michael Troller. How the Internet Works, Eighth Edition. Eigth ed. Que, O'Reilly Media, (2006)

[46] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. IEEE, 2005.

[47] R. Blaha-R. Marko-A. Zellhofer/H. Liebel. „Rechtsfragen des Cloud Computing.“ Medien und Recht Verlag, (2011)

[48] Recordon, David, and Drummond Reed. "OpenID 2.0: a platform for user-centric identity management." Proceedings of the second ACM workshop on Digital identity management. (2006): 11-16

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[49] Reiche, Albert. "Http distributed remote user authentication system." U.S. Patent No. 6,092,196. 18 Jul. 2000.

[50] Rhea, Sean, et al. "OpenDHT: a public DHT service and its uses." Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications. 2005.

[51] Riss in Kletečka/Schauer, ABGB-ON 1.02

[52] Rosenblatt, Bill, Bill Trippe, and Stephen Mooney. "Digital Rights Management." New York (2002).

[53] Rountree, Derrick, Castrillo, Ileana, and Jiang, Hai. „The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.“ Amsterdam: Syngress, an Imprint of Elsevier, (2014)

[54] Rowstron, Antony, and Peter Druschel. "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems." IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing. Springer, Berlin, Heidelberg, 2001.

[55] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: what it is, and what it is not." 2015 IEEE Trustcom/BigDataSE/ISPA. Vol. 1. IEEE, 2015.

[56] Saini, Baljit Singh, and Anju Bala. "A review of bot protection using captcha for web security." IOSR Journal of Computer Engineering 8.6 (2013): 36-42.

[57] Samani, Raj, Honan, Brian, Reavis, Jim, Jirasek, Vladimir, Katsaropoulos, Chris, Rearick, Benjamin, Govindaradjane, Punithavathy, and Rogers, Mark. „CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security.“ Waltham, Maryland: Elsevier : Syngress, (2015)

[58] Sandhu, Ravi S., et al. "Role-based access control models." Computer 29.2 (1996): 38-47

[59] Stephan Kolter. „Digital Rights Management: Eine Lösung für die digitale Krise des Urheberrechts?“ VDM Verlag Dr. Müller (2008)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[60] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

[61] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

[62] Talukder, Asoke K., and Lawrence Zimmerman. "Cloud economics: Principles, costs, and benefits." Cloud computing. Springer, London, (2010)

[63] Tang, Changlong, and Jiqiang Liu. "Selecting a trusted cloud service provider for your SaaS program." Computers & Security 50 (2015)

[64] Tang, Yang, et al. "Secure overlay cloud storage with access control and assured deletion." IEEE Transactions on dependable and secure computing 9.6 (2012): 903-916

[65] Venkatesan, Ramarathnam, et al. "Robust image hashing." Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101). Vol. 3. IEEE, (2000): 664 -666

[66] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I)

[67] Vossen, Gottfried, Till Haselmann, and Thomas Hoeren. „Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte.“ Dpunkt. verlag, (2013)

[68] Wang, Xin, et al. "The MPEG-21 rights expression language and rights data dictionary." IEEE Transactions on Multimedia 7.3 (2005): 408-417.

[69] Welser/Zöchling-Jud. „Bürgerliches Recht II.“ MANZ Verlag Wien (2015)

[70] Xing, Yuping, and Yongzhao Zhan. "Virtualization and cloud computing." Future Wireless Networks and Information Systems. Springer, Berlin, Heidelberg, (2012)

[71] Zeng, Lingfang, et al. "Safevanish: An improved data self-destruction for protecting data privacy." 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE, 2010.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

5.2 Rechtsgrundlagen & Relevante Judikatur

[1] ABGB - Allgemeines Bürgerliches Gesetzbuch

[2] BGH, Urteil vom 15.11.2006, Az. XII ZR 120/04 = MMR 2007

[3] EU-Datenschutzrichtlinie (Richtlinie 95/46/EG)

[4] Entscheidung des OGH RS0130905. GZ 6 Ob 23/16z. (20.07.2016)

[5] Europäisches Parlament und Rat. VERORDNUNG (EU) 2016/679 (Datenschutz-Grundverordnung) DSGVO

[6] Charta der Grundrechte der Europäischen Union

[7] Die Europäische Menschenrechtskonvention

[8] European Commission - Standard Contract Clauses (SCC)

[9] EuGH C-131/12

[10] EuGH C362/14

[11] OECD „Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten“.

[12] UNO „Resolution der Generalversammlung 217 A(III). Allgemeine Erklärung der Menschenrechte“.

5.3 Zeitungsartikel und Presse

[1] ComputerWeekly. „A history of cloud computing.“ http://www.computerweekly.com/feature/A-history-of-cloud-computing (zugegriffen: 1.2.2020)

[2] Gerichtshof der Europäischen Union. „Pressemitteilung Nr. 70/14 - Urteil in der Rechtssache C-131/12“ http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (zugegriffen: 02.06.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[3] Gerichtshof der Europäischen Union. „Pressemitteilung Nr. 7/18.“ https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-01/cp180007de.pdf (zugegriffen: 01.11.2020)

[4] Tony Baer, “Finding the data buried in cloud storage” https://www.zdnet.com/article/finding-the-data-buried-in-cloud-storage/ (zugegriffen: 10.09.2020)

[5] Viktor Mayer-Schönberger. „Interview: Daten brauchen ein Verfallsdatum“ http://www.golem.de/0804/58721.html (zugegriffen:15.8.2019)

[6] ZackZack.at. „6 JAHRE NACH SCHREMS-KLAGE.„ https://zackzack.at/2020/07/01/6-jahre-nach-schrems-klage-facebook-urteil-veraergert-datenschuetzer/ (zugegriffen: 01.11.2020)

5.4 Internet

[1] AICPA. „American Institute of Certified Public Accountants.“ https://www.aicpa.org/ (zugegriffen: 1.2.2020)

[2] AICPA. “System and Organization Controls: SOC Suite of Services.” https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html (zugegriffen. 1.5.2020)

[3] „Amazon.com“ https://www.amazon.com/ (zugegriffen: 27.10.2020)

[4] „Amazon Web Services (AWS).“ https://aws.amazon.com/ (zugegriffen: 1.5.2020)

[5] AWS. „AWS GovCloud (US)“. https://aws.amazon.com/govcloud-us/ (zugegriffen: 27.19.2020)

[6] AWS. „Amazon Web Services AWS“. https://aws.amazon.com/ (zugegriffen: 27.10.2020)

[7] AWS. „Hybrid Cloud.“ https://aws.amazon.com/hybrid/ (zugegriffen: 27.10.2020)

[8] „Benjamin Black – EC2 Origins.“ http://blog.b3k.us/2009/01/25/ec2-origins.html (zugegriffen: 1.5.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[9] CCITT. „INFORMATION TECHNOLOGY – DIGITAL COMPRESSION AND CODING OF CONTINUOUS-TONE STILL IMAGES – REQUIREMENTS AND GUIDELINES“ http://www.w3.org/Graphics/JPEG/itu-t81.pdf (zugegriffen: 1.3.2020)

[10] Cloudiax. „Contract terms for licensing of cloud services.“ https://www.cloudiax.com/contract-terms/ (zugegriffen: 28.10.2020)

[11] Cloud Industry Forum. „8 criteria to ensure you select the right cloud service provider“ https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider (zugegriffen: 20.10.2020)

[12] Cloud Security Alliance. „Security Guidance.“ https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf (zugegriffen: 1.10.2020)

[13] CSA. „Cloud Security Alliance.“ https://cloudsecurityalliance.org (zugegriffen: 1.2.2020)

[14] CSA. „CSA-Guidance.“ https://github.com/cloudsecurityalliance/CSA-Guidance (zugegriffen: 1.2.2020)

[15] CSA. „CSA Security Trust Assurance and Risk (STAR).“ https://cloudsecurityalliance.org/star/ (zugegriffen: 1.2.2020)

[16] CSA. „Open Certification Framework“ https://cloudsecurityalliance.org/star/levels/ (zugegriffen: 1.2.2020)

[17] CSA. „Cloud Controls Matrix (CCM)“ https://cloudsecurityalliance.org/research/cloud-controls-matrix/ (zugegriffen: 1.2.2020)

[18] CSA. „Working Group Consensus Assessments.“ https://cloudsecurityalliance.org/group/consensus-assessments/ (zugegriffen: 1.2.2020)

[19] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. „Internationaler Datentransfer.“ https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Internationaler_Datentransfer.html (zugegriffen: 29.10.2020)

[20] DLA PIPER. „Data Protection Laws of the world.” https://www.dlapiperdataprotection.com/ (zugegriffen: 29.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[21] Europe v Facebook. „Sammelklage gegen Facebook eingebracht.“ http://www.europe-v-facebook.org/sk/pa_de.pdf (zugegriffen 9.9.2020)

[22] Google. „Google Workspace.“ https://workspace.google.com/ (zugegriffen: 27.10.2020)

[23] Google. „Google Cloud“. https://cloud.google.com/ (zugegriffen: 27.10.2020)

[24] Instagram. „Instagram.“ https://www.instagram.com/ (zugegriffen: 1.2.2020)

[25] ISO.org. „ISO.“ https://www.iso.org/home.html (zugegriffen: 20.10.2020)

[26] ISO. “ISO/IEC 27001 Information Security Management.” https://www.iso.org/isoiec-27001-information-security.html (zugegriffen: 20.10.2020)

[27] ISO. “ISO/IEC 27018:2019 Information Technology – Security techniques.” https://www.iso.org/standard/76559.html (zugegriffen: 20.10.2020)

[28] ISO.org “The ISO Survey of Management System Standard Certifications.” https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2 (zugegriffen: 1.2.2020)

[29] ISO. „ISO/IEC 27002:2013“ http://www.iso27001security.com/html/27002.html (zugegriffen: 1.2.2020)

[30] Kompetenzzentrum Trusted Cloud. „Leitfaden – Vertragsgestaltung beim Cloud Computing Nr 3.“ https://www.trusted-cloud.de/sites/default/files/ap_3_vertragsleitfaden.pdf (zugegriffen: 01.06.2020

[31] Microsoft. „Azure Government“. https://azure.microsoft.com/en-us/global-infrastructure/government/ (zugegriffen: 27.10.2020)

[32] Microsoft. „Microsoft Azure“. https://azure.microsoft.com/ (zugegriffen: 27.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[33] Microsoft. „Hyper-V“. https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v (zugegriffen: 27.10.2020)

[34] Microsoft. „Azure Hybrid Cloud.“ https://azure.microsoft.com/en-us/solutions/hybrid-cloud-app/ (zugegriffen: 27.10.2020)

[35] Microsoft. „Office 365“. https://www.office.com/ (zugegriffen: 27.1.2020)

[36] NetApp. „Hybrid Cloud.“ https://www.netapp.com/hybrid-cloud/ (zugegriffen: 27.10.2020)

[37] „OAuth 2.0“ https://oauth.net/2/ (zugegriffen: 1.2.2020)

[38] Office 365. „Data Classification Overview.“ https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide (zugegriffen: 9.09.2020)

[39] OpenID. „OpenID Connect“ https://openid.net/connect/ (zugegriffen: 1.2.2020)

[40] OpenID. „OpenID Foundation.“ https://openid.net/foundation/ (zugegriffen: 1.2.2020)

[41] Oasis. „SAML v2.0 Errata“ http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0-cd-02.html (zugegriffen: 1.2.2020)

[42] RedHat. „Enterprise Virtualization“. https://www.redhat.com/en/technologies/virtualization/enterprise-virtualization (zugegriffen: 27.10.2020)

[43] SAP. „SAP Cloud Platform“. https://www.sap.com/products/cloud-platform.html (zugegriffen: 27.10.2020)

[44] „vmware“. https://www.vmware.com/ (zugegriffen: 27.10.2020)

[45] Wirtschaftsagentur Wien (Hrsg: Paul Meinl). „Software as a service, Verträge richtig abschließen.“ 2 Aufl., http://www.it-lab.at/__docs/SaaS-Leitfaden__31.pdf (zugegriffen: 6.10.2019)

[46] WKO.at. „EuGH: EU-US Privacy-Shield ungültig“, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-US-Privacy-Shield.html (zugegriffen: 29.10.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

[47] W3C. „Web Authentication: An API for accessing Public Key Credentials” https://www.w3.org/TR/webauthn/ (zugegriffen: 1.2.2020)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 6
Abbildungsverzeichnis

Abbildung 1: Einteilung von Cloud-Service-Modellen 7
Abbildung 2: Referenz und Architektur Modell 16
Abbildung 3: Übersicht des Datenschutzes Weltweit 33
Abbildung 4: Übersicht der Standards und Frameworks 39
Abbildung 5: Beziehungen der unterschiedlichen Frameworks 40
Abbildung 6: Übersicht der ISO Zertifizierungen 41
Abbildung 7: Übersicht ISO 27001 Standard 42
Abbildung 8: Verbreitung von ISO 27001 44
Abbildung 9: Übersicht Open Certification Framework 49
Abbildung 10: X-pire! Architektur 84
Abbildung 11: X-Pire 2.0 publizieren von Daten 87
Abbildung 12: DRS Protokoll Übersicht 100
Abbildung 13: Prozess zur Überprüfung von digitalen Wasserzeichen 106
Abbildung 14: DRM-System - Prozessübersicht 108
Abbildung 15: Actor Modell 111
Abbildung 16: System Architektur 112

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kapitel 7
Tabellenverzeichnis

Tabelle 1 IaaS Aufgabenverteilung 8
Tabelle 2 IaaS Vor- und Nachteile 8
Tabelle 3 PaaS Aufgabenverteilung 9
Tabelle 4 PaaS Vor- und Nachteile 10
Tabelle 5 SaaS Aufgabenverteilung 11
Tabelle 6 SaaS Vor- und Nachteile 11
Tabelle 7 SOC Übersicht 47
Tabelle 8 Übersicht weltweiter Standards und Zertifizierungen 57

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.