Zürcher Hochschule für Angewandte Wissenschaften
School of Management and Law

Masterarbeit

Confidential Computing – Eine Chance für die datenschutzkonforme Ausgestaltung von risikoreichen Datenbearbeitungen?

Betreuungsperson:
Frau Prof. Ursula Sury

Vorgelegt von:
Adrienne Remund
Matrikelnummer: 13-104-047

ZHAW Winterthur
Eingereicht am: 30. Mai 2023

Management Summary

Seit der Jahrtausendwende ist die Zunahme leistungsfähiger IT-Infrastrukturen und die Beschaffung und Analyse von grossen Datenmengen klar erkennbar. Die Vertrauenswürdigkeit und die Integrität von IT-Infrastrukturen und Daten waren und sind zentrale Themen. Bereits damals wurde mit Trusted Computing eine Technologie eingeführt, um die Vertrauenswürdigkeit eines Computersystems zu gewährleisten. Dazu wird eine Vertrauenskette zwischen der Hardware und dem Betriebssystem geschaffen, welche vor bösartigen Plattformmanipulationen schützt. Diese Technologie wird heutzutage standardmässig eingesetzt. Durch die zunehmende digitale Vernetzung, insbesondere die Speicherung und Bearbeitung von personenbezogenen Daten innerhalb einer Cloud, haben sich neue rechtliche Anforderungen hinsichtlich der Datenbearbeitung ergeben. Trusted Computing allein ist längst nicht mehr ausreichend. Eine Auslagerung von Daten bringt immer einen Kontrollverlust mit sich. Einerseits kann der Serverstandort des Anbieters datenschutzrechtlich hohe Risiken für die Privatsphäre der betroffenen Person auslösen, da der Datenschutz international unterschiedlich ausgelegt wird. Zum anderen ist die Art des genutzten Cloud-Services ausschlaggebend. Werden in einer Cloud lediglich personenbezogene Daten gespeichert, können Verantwortliche diese durch Verschlüsselung vor Zugriff schützen. Werden Daten jedoch in einer Cloud bearbeitet, braucht der Anbieter vollen Zugriff auf die Daten. Diese Zugriffsrisiken können nicht mit jeder Art von personenbezogenen Daten, insbesondere besonders schützenswerte Daten, vereinbart werden. Confidential Computing bietet als innovative Technologie in dieser Hinsicht eine Lösung. Während Trusted Computing den Fokus auf der Vertrauenswürdigkeit der Plattform selbst hat, setzt Confidential Computing bei der Vertraulichkeit der Datenbearbeitung an. Es handelt sich um ergänzende Technologien. Die Forschungsarbeit zeigt auf, dass mit Confidential Computing eine isolierte Enklave eingeführt wird, welche die Möglichkeit bietet, risikoreiche Datenbearbeitungen durchzuführen, welche bisher nicht datenschutzkonform ausgeführt werden konnten. Der Schutz der Daten wird zu jederzeit – auch in einer Cloud – gewährleistet und der Zweck der Datenbearbeitung wird im Voraus technisch definiert. Die Technologie findet namentlich in der Gesundheits- und Marketingbranche sowie in der Nutzung von Sekundärdaten Anwendung. Dazu benötigt es praktikable, regulatorische Bestimmungen und Best-Practice-Beispiele, welche mehr Klarheit sowie Vertrauen in die Technologie schaffen.

Management Summary

Since the turn of the millennium, the increase in powerful IT infrastructures and the acquisition and analysis of large amounts of data has been clearly visible. The trustworthiness and integrity of IT infrastructures and data were and are central issues. Already at that time, a technology was introduced with Trusted Computing to guarantee the trustworthiness of a computer system. For this purpose, a chain of trust is created between the hardware and the operating system, which protects against malicious platform manipulation. This technology is used by default today. The increasing digital networking, especially the storage and processing of personal data within a cloud, has resulted in new legal requirements with regard to data handling. Trusted computing alone is no longer sufficient. Outsourcing data always entails a loss of control. On the one hand, the server location of the provider can trigger high risks for the privacy of the person concerned in terms of data protection law, as data protection is interpreted differently internationally. On the other hand, the type of cloud service used is decisive. If only personal data is stored in a cloud, data controllers can protect it from access through encryption. However, if data is processed in a cloud, the provider needs full access to the data. These access risks cannot be reconciled with every type of personal data, especially data requiring special protection. Confidential computing, as an innovative technology, offers a solution in this regard. While Trusted Computing focuses on the trustworthiness of the platform itself, Confidential Computing focuses on the confidentiality of data processing. These are complementary technologies. The research paper shows that Confidential Computing introduces an isolated enclave that offers the possibility of performing risky data processing that could not previously be accomplished in accordance with data protection. Data protection is guaranteed at all times - even in a cloud - and the purpose of the data processing is technically defined in advance. The technology is used particularly in the health and marketing sectors as well as in the use of secondary data. This requires practicable regulatory provisions and best-practice examples that create more clarity and trust in the technology.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
Abs.	Absatz
AMD	Advanced Micro Devices
ARM	Acorn RISC Machine
Art.	Artikel
Aufl.	Auflage
Bsp.	Beispiel
bspw.	beispielsweise
BV	Bundesverfassung
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CPU	Central Processing Unit
d.h.	das heisst
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz) vom 19. Juni 1992 (Stand am 1. März 2019, Aufhebungsdatum: 1. September 2023) 235.1.
nDSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz) vom 25. September 2020 (Stand am 1. September 2023) 235.1.
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
DSV	Verordnung über den Datenschutz (Datenschutzverordnung, DSV) vom 31. August 2022.
etc.	et cetera
EDPS	European Data Protection Supervisor
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäische Menschenrechtskonvention
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU	Europäische Union
EWR	Europäischer Währungsraum
EuGH	Europäischer Gerichtshof

HFG	Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz) vom 30. September 2011 (Stand am 1. Dezember 2022)
Hrsg.	Herausgeber
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
Intel SGX	Intel Software Guard Extensions
i.S.	im Sinne
i.S.v.	im Sinne von
IT	Informations-Technologie
Kap.	Kapitel
lit.	litera
NIST	National Institute of Standards and Technology
PS-Regime	Privacy Shield Regime
PwC	PricewaterhouseCoopers
resp.	respektive
N	Randnote
S.	Seite
s.	siehe
SCC	Standard Contractual Clause (Standardvertragsklauseln)
Schrems II-Urteil	EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ltd, Maximilian Schrems.
SEV	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten Straßburg/Strasbourg, 28.I.1981.
SGX	Software Guard Extensions
sog.	sogenannt
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 23. Januar 2023), 311.0
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TEE	Trusted Executions Environment
TIA	Transfer Impact Assessment

TOM	technische und organisatorische Massnahmen
TPM	Trusted Platform Module
TwC	Trustworthy Computing
u.a.	unter anderem
US	Vereinigte Staaten
USA	Vereinigte Staaten von Amerika
u.U.	unter Umständen
vgl.	vergleiche
VPN	Virtual Private Network
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
zit.	zitiert

Literaturverzeichnis

ABDULLAH LAMYA/FREILING FELIX/QUINTERO JUAN/ BENENSON ZINAIDA, Sealed Computation: Abstract Requirements for Mechanisms to Support Trustworthy Cloud Computing, in: Katsikas Sokratis K./Cuppens Frédéric/Cuppens Nora/Lambrinoudakis Costas/ Antón Annie/Gritzalis Stefanos/Mylopoulos John/Kalloniatis Christos (Hrsg.), Computer Security ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Switzerland 2019, S. 137-152.

BERANEK ZANON NICOLE/DE LA CRUZ BÖHRINGER CARMEN, Urheberrechtliche Beurteilung von IaaS- (und XaaS)- Cloud-Diensten für die betriebliche Nutzung gemäss Art. 19 URG, in: Amstutz Marc/Berger Mathis/Borer Jürg/La Spada Anne-Virginie/Mathys Roland/Picht Peter Georg/Rigamonti Cyrill P./Thouvenin Florent/de Werra Jacques/Wild Gregor (Hrsg.), Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht, 2013, S. 663-681.

BLONSKI DOMINIKA, Cloud Computing - Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, in: Epiney Astrid/Rovelli Sophia, Künstliche Intelligenz und Datenschutz / L'intelligence artificielle et protection des données, Forum Europarecht, 2021, S. 65-80.

BRANDL HANS, Trusted Computing Grundlagen, in: Pohlmann N./Reimer H. (Hrsg.), Trusted Computing – Ein Weg zu neuen IT-Sicherheitsstrukturen, 1. Aufl., Wiesbaden 2008, S. 21-42.

ECKERT MARTIN/IMFELD TABEA, Datenschutzzertifizierungen in der Schweiz, in: Recht relevant. für Compliance Officers, Schulthess Juristische Medien (Hrsg.), März 2022, S. 12.

HALBHEER ROGER, Microsofts Trustworthy Computing, in: Baeriswyl Bruno/Rudin Beat/Hämmerli Bernhard M./Schweizer Rainer J./Karjoth Günter/Vasella David (Hrsg.), Zeitschrift für Datenrecht und Informationssicherheit, 2005, S. 124-127.

HÄDER MICHAEL, Empirische Sozialforschung – Eine Einführung. 4. Aufl., Wiesbaden 2019.

HELFFERICH CORNELIA, Leitfaden- und Experteninterviews, in: Baur Nina/Blasius Jörg, Handbuch Methoden der empirischen Forschung, Wiesbaden 2022, S. 875-892.

HERFERT MICHAEL/LANGE BENJAMIN/SPYCHALSKI DOMINIK, Verschlüsselung in der Cloud, in: Baeriswyl Bruno/Rudin Beat/Hämmerli Bernhard M./Schweizer Rainer J./Karjoth Günter/Vasella David (Hrsg.), Zeitschrift für Datenrecht und Informationssicherheit, 2019, S. 128-133.

HOFFMANN RAUNO, Cloud Computing: Die Nutzung von Cloud-Computing – Services und deren datenschutzrechtliche Voraussetzungen, in: Der Schweizer Treuhänder, Zürich 2012, S. 465–469.

HOPF WULF, Christel Hopfs Schriften zu Methodologie und Methoden im Kontext ihres wissenschaftlichen Werdegangs, in: Hopf Christel, Schriften zu Methodologie und Methoden qualitativer Sozialforschung, Wiesbaden 2016, S. 1-12.

HÜRLIMANN DANIEL/STEIGER MARTIN, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz, in: Schweizerischer Anwaltsverband (Hrsg.), Anwaltsrevue: Das Praxismagazin des schweizerischen Anwaltsverbandes, 2021, S. 199-205.

JÄGER HUBERT/RIEKEN RALF/ERNST EDMUND, Herausforderung Datenschutz und Datensicherheit in der Cloud, in: Jäger Hubert/Rieken Ralf (Hrsg.), Manipulationssichere Cloud-Infrastrukturen – Nachhaltige Digitalisierung durch Sealed Cloud Security, Wiesbaden 2020, S. 3-33 (zit. als JÄGER/RIEKEN/ERNST, Herausforderung Datenschutz, S. x).

JÄGER HUBERT/RIEKEN RALF/ERNST EDMUND/MONITZER ARNOLD/NGUYEN DAU KHIEM/ MODI JAYMIN/ ANTONY SIBI/KARATZAS CHRISTOS/ STARK FRANZ/ FIETZ JARO/ABDULLAH LAMYA, Grundprinzip der Sealed Cloud, in: Jäger Hubert/Rieken Ralf (Hrsg.), Manipulationssichere Cloud-Infrastrukturen – Nachhaltige Digitalisierung durch Sealed Cloud Security, Wiesbaden 2020, S. 33-78 (zit. als, JÄGER et al., Grundprinzip der Sealed Cloud, S. x).

JÄGER HUBERT/RIEKEN RALF/MONITZER ARNOLD, Wie viel Sicherheit ist genug?, in: Jäger Hubert/Rieken Ralf (Hrsg.), Manipulationssichere Cloud-Infrastrukturen – Nachhaltige Digitalisierung durch Sealed Cloud Security, Wiesbaden 2020, S. 167-185 (zit. als, JÄGER et al., Wie viel Sicherheit ist genug?, S. x).

MÜLLER THOMAS, Trusted Computing Systeme – Konzepte und Anforderungen, Berlin Heidelberg 2008.

POHLMANN NORBERT, Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 2. Aufl., Wiesbaden 2022 (zit. als POHLMANN, S. x).

POHLMANN NORBERT, Die Vertrauenswürdigkeit von Software, in: Datenschutz und Datensicherheit, Oktober 2014. S. 655–659 (zit. als POHLMANN, Die Vertrauenswürdigkeit von Software, S. x).

ROHR SEBASTIAN, Trusted Computing und die Umsetzung in heutigen Betriebssystemen, in: Pohlmann N./Reimer H. (Hrsg.), Trusted Computing – Ein Weg zu neuen IT-Sicherheitsstrukturen, 1. Aufl., Wiesbaden 2008, S. 57-70.

ROSTEK THOMAS, Die Trusted Computing Group, in: Pohlmann N./Reimer H. (Hrsg.), Trusted Computing – Ein Weg zu neuen IT-Sicherheitsstrukturen, 1. Aufl., Wiesbaden 2008.

SCHLÜTER JAN/TEUFEL STEPHANIE, Cloud Computing - Anwendungen im Netz - Der nächste Hype steht in den Startlöchern: Verteilte Anwendungen im Netz werden zur Wolke, in: in: Baeriswyl Bruno/Rudin Beat/Hämmerli Bernhard M./Schweizer Rainer J./Karjoth Günter/Vasella David (Hrsg.), Zeitschrift für Datenrecht und Informationssicherheit, 2009, S. 6-9.

SCHOLL ARMIN, Die Befragung, 4. Aufl., München 2018.

SCHÖNBÄCHLER MATTHIAS R., Zum neuen Datenschutzrecht, in: Schmid Jörg/Krauskopf Frédéric, Zeitschrift des Bernischen Juristenvereins, 159/2023, S. 171-195.

SEGALL ARIEL, Trusted Platform Modules – Why, when and how to use them, in: The Institution of Engineering and Technology (Hrsg.), IET Professional Applications of Computing, Bd. 13, London 2016.

STECKLER BRUNHILDE/KREMPEL ERIK, «Privacy by Design» im Dialog von Recht und Technik. in: Gransche, B., Manzeschke, A. (Hrsg.) Das geteilte Ganze, Springer, Wiesbaden 2020, S. 79 f.

WASSERMANN SANDRA, Das qualitative Experteninterview, in: Miederberger Marlen/Wassermann Sandra (Hrsg.), Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung, Wiesbaden 2015, S. 51-65.

WEISS BERNARD, TPM Key Management, in: Pohlmann N./Reimer H. (Hrsg.), Trusted Computing – Ein Weg zu neuen IT-Sicherheitsstrukturen, 1. Aufl., Wiesbaden 2008, S. 140-155.

Materialien

BUNDESAMT FÜR JUSTIZ (BJ), Bericht zum US Cloud Act - Gutachten des Bundesamts für Justiz vom 17. September 2021, https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html, besucht am: 26.03.2023 (zit. als BJ, S. x).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Das neue Datenschutzgesetz aus Sicht des EDÖB, 27.10.2022, https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/20210305_ndsg_sicht_edoeb.html, besucht am: 26.03.2023 (zit als, EDÖB, Das nDSG aus Sicht des EDÖB).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge, 27.08.2021, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html, besucht am: 27.03.2023 (zit. als EDÖB, Die Übermittlung von Personendaten, S. x).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Stärkung des Datenschutzes, https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html, besucht am: 28.05.2023 (zit. als EDÖB, Stärkung des Datenschutzes, Worum geht es?).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Datenschutz, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html, besucht am: 24.03.2023 (zit. als EDÖB, Datenschutz)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Erläuterungen zu Cloud Computing, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html, besucht am: 14.03.2023 (zit. als EDÖB, Erläuterungen zu Cloud Computing).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Tipps zur DSGVO, https://www.edoeb.admin.ch/edoeb/de/home/aktuell/rgpd-last-minute.html#:~:text=Als%20Schweizer%20Unternehmen%20gilt%20f%C3%BCr,bearbeiten%20(Datenschutzerkl%C3%A4rung%2C%20AGB).&text=Die%20DSGVO%20ist%20nicht%20direkt%20auf%20Schweizer%20Unternehmen%20anwendbar, besucht am: 25.03.2023 (zit. als EDÖB, Tipps zur DSGVO).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Übermittlung ins Ausland, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html, besucht am: 26.03.2023 (zit. als EDÖB, Übermittlung ins Ausland).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, 08.09.2020, https://www.newsd.admin.ch/newsd/message/attachments/64258.pdf, besucht am: 24.03.2023 (zit. als EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA, S. x).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Datenschutz und Forschung im Allgemeinen, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/statistik--register-und-forschung/forschung/datenschutz-und-forschung-im-allgemeinen.html, besucht am: 26.03.2023 (zit. als EDÖB, Datenschutz und Forschung im Allgemeinen).

EIDGENÖSSISCHES DEPARTEMENT FÜR WIRTSCHAFT, BILDUNG UND FORSCHUNG (WBF), Neues Datenschutzgesetz (revDSG), https://www.kmu.admin.ch/kmu/de/home/fakten-trends/digitalisierung/datenschutz/neues-datenschutzgesetz-rev-dsg.html, besucht am: 24.03.2023 (zit. als WBF, Neues Datenschutzgesetz (revDSG).

EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT (EJPD), Verordnung über den Datenschutz (Datenschutzverordnung, DSV) – Erläuternder Bericht, 31.08.2022, https://www.newsd.admin.ch/newsd/message/attachments/75623.pdf, besucht am: 27.03.2023 (zit. als EJPD, S. x).

EUROPÄISCHE KOMMISSION, Was bedeutet „Datenschutz durch Technikgestaltung“ und „durch datenschutzfreundliche Voreinstellungen“?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_de, besucht am: 24.03.2022 (zit. als Europäische Kommission, Was bedeutet „Datenschutz durch Technikgestaltung“ und „durch datenschutzfreundliche Voreinstellungen“?).

KOMMISSION FÜR WISSENSCHAFT, BILDUNG UND KULTUR, Mo. Ständerat (WBK-SR). Rahmengesetz für die Sekundärnutzung von Daten, 21.04.2023, https://www.parlament.ch/centers/kb/Documents/2022/Kommissionsbericht_WBK-N_22.3890_2023-04-21.pdf, besucht am: 22.05.2023.

Internetquellen

ACHEMLAL MOHAMMED/BOUABDALLAH ABDELMADJID/SABT MOHAMED, Trusted Execution Environment: What It Is, and What It Is Not, in: IEEE Computer Society, 2015, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7345265&tag=1, besucht am: 24.02.2023, S. 57-64.

AMD, Secure Encrypted Virtualization (SEV), https://www.amd.com/en/developer/sev.html, besucht am: 26.03.3023.

ARM DEVELOPER, ARM Security Technology Building a Secure System using TrustZone® Technology, April 2009, https://developer.arm.com/documentation/PRD29-GENC-009492/latest/, besucht am: 11.03.2023 (zit. als ARM, Building a Secure System, S. x).

ARM Developer, Security in an ARMv8 System, März 2017, https://developer.arm.com/documentation/100935/0100/The-TrustZone-hardware-architecture-, besucht am: 11.03.2023 (zit. als ARM, Security in an ARMv8 System, S. x).

BERN UNIVERSITY OF APPLIED SCIENCES, School of Engineering and Computer Science Hardware Protected Confirmation, https://www.bfh.ch/en/research/reference-projects/hardware-protected-confirmation/, besucht am: 05.03.2023 (zit. als Bern University of Applied Sciences, Course of Action).

BUNDESKARTELLAMT, Prüfung Microsofts marktübergreifender Bedeutung, 28.03.2023, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/28_03_2023_Microsoft.html, besucht am: 24.04.2023 (zit. als Bundeskartellamt, Prüfung Microsofts marktübergreifender Bedeutung).

CONFIDENTIAL COMPUTING CONSORTIUM (CCC), About the Confidential Computing Consortium, https://confidentialcomputing.io/about/, besucht am: 24.02.2023 (zit. als CCC, About the Confidential Computing Consortium).

CONFIDENTIAL COMPUTING CONSORTIUM (CCC), Confidential Computing: Hardware-Based Trusted Execution for Applications and Data, November 2022, https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf, besucht am: 24.01.2023 (zit. als CCC, Hardware-Based Trusted Execution for Applications and Data, S. x).

CONFIDENTIAL COMPUTING CONSORTIUM (CCC), A Technical Analysis of Confidential Computing, November 2022, https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf, besucht am: 27.02.2023 (zit. als CCC, A Technical Analysis of Confidential Computing, S. x).

COSTAN VICTOR/DEVADAS SRINIVAS, Intel SGX Explained, Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology, https://eprint.iacr.org/2016/086.pdf, besucht am: 12.03.2023 (zit. als COSTAN/DEVADAS, S. x).

COVIELLO MICHELE, «Es sieht relativ ernst aus»: Ein massiver Cyberangriff trifft die Universität Zürich, in: Neue Zürcher Zeitung, 02.02.2023, https://www.nzz.ch/zuerich/massiver-cyberangriff-gegen-die-universitaet-zuerich-it-kann-die-angriffe-bisher-abwehren-ld.1724389, besucht am: 27.02.2023 (zit. als COVIELLO, Massiver Cyberangriff trifft die Universität Zürich).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Der EDÖB – Auftrag & Aufgaben: Der Datenschutz, https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/auftragundaufgaben-DS.html, besucht am: 15.05.2023 (zit. als EDÖB, Auftrag & Aufgaben)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Aufgaben des EDÖB, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/aufgaben-des-edoeb.html, besucht am: 25.03.2023 (zit. als EDÖB, Aufgaben des EDÖB).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Bundesverwaltung führt Public Cloud gestützte Anwendung Microsoft 365 ein, 07.03.2023, https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#207406292, besucht am: 10.04.2023 (zit. als EDÖB, Bundesverwaltung führt Public Cloud gestützte Anwendung Microsoft 365 ein).

EUROPEAN DATA PROTECTION SUPEREVISOR (EDPS), Datenschutz-Folgenabschätzung (DSFA), https://edps.europa.eu/data-protection/our-role-supervisor/data-protection-impact-assessment-dpia_de, besucht am: 24.04.2023 (zit. als EDPS, Datenschutz-Folgenabschätzung).

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), Datenverarbeitung dokumentieren: Der EDSB-Leitfaden zur Sicherstellung der Rechenschaftspflicht, https://edps.europa.eu/sites/edp/files/publication/18-12-11_factsheet3_documenting_data_processing_de.pdf.pdf, besucht am: 16.03.2023 (zit. als EDPS, Datenverarbeitung dokumentieren, S. x).

EUROPÄISCHE KOMMISSION, Gemeinsame Erklärung der Europäischen Kommission und der Vereinigten Staaten zum Transatlantischen Datenschutzrahmen, 25.03.2022, https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087, besucht am: 24.04.2023 (zit. als Europäische Kommission, Transatlantischer Datenschutzrahmen).

GARTNER, Gartner Identifies the Top Strategic Technology Trends for 2022, 18.10.2021, https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022, besucht am: 25.02.2023 (zit. als Gartner, Top Strategic Technology Trends for 2022).

GÜNTNER JOACHIM, Bücher in der Wolke – Wie sich Google unsere Bibliothek denkt, In: NZZ Zeitungsarchiv, 13.08.2009, https://zeitungsarchiv.nzz.ch/read/125950/125950/2009-08-13/37, besucht am: 27.02.2023.

HÄBERLI STEFAN, Der neue Swisscom-Chef muss sein Glück in der Cloud suchen, in: Neue Zürcher Zeitung, 28.04.2022, https://www.nzz.ch/wirtschaft/neuer-swisscom-ceo-christoph-aeschlimann-sucht-weg-aus-hamsterrad-ld.1681541, besucht am: 27.02.2023 (zit. als HÄBERLI, Der neue Swisscom-Chef, 2022).

HÄBERLI STEFAN, Die umstrittenen Verträge mit ausländischen Cloud-Anbietern sind unter Dach und Fach, in: Neue Zürcher Zeitung, 27.09.2022, https://www.nzz.ch/wirtschaft/cloud-vertraege-mit-amazon-alibaba-co-sind-unterschrieben-ld.1704527, besucht am: 28.02.2023 (zit. als HÄBERLI, Die umstrittenen Verträge, 2022).

HUMBY AND DUNN, http://www.humbyanddunn.com/, besucht am: 27.02.2023.

INTEL, Trusted-Platform-Modul (TPM) – Überblick, o.D., https://www.intel.de/content/www/de/de/business/enterprise-computers/resources/trusted-platform-module.html#:~:text=Ein%20TPM%20ist%20eine%20Sicherheitshardware,PCs%20k%C3%B6nnen%20TPM%202.0%20unterst%C3%BCtzen, besucht am: 06.03.2023 (zit. als Intel, Trusted-Platform-Modul (TPM) – Überblick).

INTEL, Intel Software Guard Extensions - Strengthen Enclave Trust with Attestation, https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/attestation-services.html, besucht am: 12.03.2023 (zit. als Intel, Remote Attestation).

KASPERSKY, Was ist Datenverschlüsselung? Definition und Erläuterung, https://www.kaspersky.de/resource-center/definitions/encryption, besucht am: 14.02.2023 (zit. als, Kaspersky, Verschlüsselung bei der Speicherung vs. Verschlüsselung bei der Übertragung).

KOHLBRENNER DAVID/SHINDE SHWETA/LEE DAYEOL/ASANOVIĆ KRSTE/SONG DAWN, Building Open Trusted Execution Environments, in IEEE Security & Privacy, Hardware-Assisted Security, https://n.ethz.ch/~sshivaji/publications/opentee_ieee-sp-magazine20.pdf, besucht am: 05.03.2023 (zit. als KOHLBRENNER et. al., S. x).

KÜDERLI URS, Im Fokus: Neue Geschäftsmodelle - Cloud Computing: Chancen nutzen und Risiken steuern, in Pricewaterhouse Cooper (PwC), Disclose: Das Onlinemagazin von PwC, https://www.pwc.ch/de/insights/disclose/22/cloud-computing-chancen-nutzen-und-risiken-steuern.html#:~:text=Cloud%20Computing%20birgt%20ein%20signifikantes,durch%20die%20Skalierbarkeit%20der%20Dienstleistungen, besucht am: 14.03.2023 (zit. als KÜDERLI, Im Fokus: Neue Geschäftsmodelle, Die wahren Vorteile der Cloud und die Nachteile).

LEXR, DSGVO und Confidential Computing, 17.01.2021, https://www.lexr.com/de-ch/blog/confidential-computing-dsgvo/, besucht am: 24.02.2023 (zit. als LEXR, DSGVO und Confidential Computing).

MCKEEN FRANK, ALEXANDROVICH ILYA/BERENZON ALEX/ROZAS CARLOS/SHAFI HISHAM/SHANBHOGUE VEDVYAS/SAVAGAONKAR UDAY, Innovative Instructions and Software Model for Isolated Execution, Intel Corporation 2013, https://www.intel.com/content/dam/develop/external/us/en/documents/hasp-2013-innovative-instructions-and-software-model-for-isolated-execution.pdf, besucht am: 12.03.2023 (zit. als MCKEEN, S. x).

MICROSOFT, European Union Model Clauses, 25.04.2023, https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses, besucht am: 17.05.2023 (zit. als Microsoft, European Union Model Clauses).

MICROSOFT, Verschlüsselung in der Cloud, 18.03.2023, https://learn.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide, besucht am: 19.03.2023 (zit. als. Microsoft, Verschlüsselung in der Cloud).

MICROSOFT, Shared responsibility in the cloud, 12.06.2022, https://learn.microsoft.com/en-gb/azure/security/fundamentals/shared-responsibility, besucht am: 19.03.2023 (zit. als Microsoft, Shared Responsibility).

MICROSOFT, Faktencheck Datenschutz: Wie wir unsere Kundendaten nach dem Schrems-II-Urteil schützen, 14.10.2021, https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/, besucht am: 22.04.2023 (zit. als Microsoft, Faktencheck).

MICROSOFT SWITZERLAND, Security-Spezialist Roger Halbheer: «Die Risiken müssen ehrlich und transparent gegeneinander abgewogen werden.», 09.03.2020, https://news.microsoft.com/de-ch/2020/03/09/die-emotionale-diskussion-bei-cloud-loesungen-muss-ernst-genommen-werden/, besucht am: 14.02.2023 (zit. als Microsoft Switzerland, Interview mit Security-Spezialist Roger Halbheer).

MICROSOFT SWITZERLAND, Wie Confidential Computing Schweizer Unternehmen zu mehr Datenschutz und Sicherheit verhilft, 26.09.2022, https://news.microsoft.com/de-ch/2022/09/26/wie-confidential-computing-schweizer-unternehmen-zu-mehr-datenschutz-und-sicherheit-verhilft/, besucht am: 24.02.2023 (zit. als Microsoft Switzerland, Wie Confidential Computing Schweizer Unternehmen zu mehr Datenschutz und Sicherheit verhilft).

MEYLE HANNES/MORAND ANNE-SOPHIE/VASELLA DAVID, DSV: keine Mindestanforderungen an die Datensicherheit, keine entsprechende Strafbarkeit, weitere Anmerkungen, 19.09.2022, https://datenrecht.ch/dsv-keine-mindestanforderungen-an-die-datensicherheit-keine-entsprechende-strafbarkeit-weitere-anmerkungen/#:~:text=mehr%20anzeigen-,DSV%3A%20keine%20Mindestanforderungen%20an%20die%20Datensicherheit,keine%20entsprechende%20Strafbarkeit%2C%20weitere%20Anmerkungen&text=An%20seiner%20Sitzung%20vom%2031,%C3%BCber%20Datenschutzzertifizierungen%20(VDSZ)%20verabschiedet, besucht am: 09.04.2023 (zit. als MEYLE/MORAND/VASELLA, S. x).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), NIST IR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases, Mai 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320.pdf, besucht am: 27.02.2023 (zit. als NIST, NIST IR 8320 Hardware-Enabled Security).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), The NIST Definition of Cloud Computing, Special Publication 800-145, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, besucht am: 12.02.2023 (zit. als NIST, Definition of Cloud Computing, S. x).

PALMER MICHAEL, Data is the New Oil, 03.11.2006, https://ana.blogs.com/maestros/2006/11/data_is_the_new.html, besucht am: 27.02.2023.

POHLMANN NORBERT, Confidential Computing, https://norbert-pohlmann.com/glossar-cyber-sicherheit/confidential-computing/, besucht am: 26.03.2023 (zit. als POHLMANN, Confidential Computing, x).

POHLMANN NORBERT, Trusted computing Base (TCB), https://norbert-pohlmann.com/glossar-cyber-sicherheit/trusted-computing-base-tcb/, besucht am: 19.02.2023 (zit. als POHLMANN, TCB).

PORTER NELLY/LUGANI SAM, Introducing Google Cloud Confidential Computing with Confidential VMs, in: Google Cloud Blog, 14.07.2020, https://cloud.google.com/blog/products/identity-security/introducing-google-cloud-confidential-computing-with-confidential-vms?hl=en, besucht am: 16.03.2023 (zit. als PORTER/LUGANI, Introducing Google Cloud Confidential Computing).

POTTI SUNIL/LUGANI SAM, How Confidential Computing can transform cloud security, in: Google Cloud Blog, 27.04.2023, https://cloud.google.com/blog/products/identity-security/rsa-confidential-computing-transforming-cloud-security?hl=en, besucht am: 15.05.2023 (zit. als POTTI/LUGANI, How Confidential Computing can transform cloud security).

ROSENTHAL DAVID, Das neue Datenschutzgesetz, in: Jusletter, 16.11.2020, https://www.rosenthal.ch/downloads/Rosenthal-revidiertesDSG.pdf, besucht am: 26.03.2023 (zit. als ROSENTHAL, N x).

RUSSINOVICH MARK, Introducing Azure confidential computing, 14.09.2017, https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/, besucht am: 16.03.2023.

SCHWEIZERISCHE AKADEMIE DER TECHNISCHEN WISSENSCHAFTEN (SATW), Empfehlungen für eine bessere Nutzung personenbezogener Daten in der Schweiz, 18.04.2023, https://www.satw.ch/fileadmin/user_upload/images/02_Themen/04_Digitalisierung/20230418_Arbeitspapier_Nutzung_personenbezogener_Daten.pdf, besucht am: 22.05.2023 (zit. als SATW, Empfehlungen, S. x).

SEAMON CHAN/TONG/KE XUE, Trusted Computing, https://cs.stanford.edu/people/eroberts/cs201/projects/trusted-computing/what.html, besucht am: 19.03.2023.

TRUSTED COMPUTING GROUP (TCG), Trusted Platform Module Library - Part 1: Architecture, Level 00 Revision 01.59, November 8, 2019, https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM2_r1p59_Part1_Architecture_pub.pdf, besucht am: 06.03.2023 (zit. als TCG, S. x).

VISCARDI REMO, Sicher in der Cloud - durch die Cloud?, in: Swiss IT Magazin, 2012, https://www.itmagazine.ch/artikel/49515/Sicher_in_der_Cloud_-_durch_die_Cloud.html, besucht am: 14.03.2023.

VASELLA TOMASO, Datenverschlüsselung in der Cloud - BYOK, BYOE, HYOK und Tokenisierung, in: Scip.ch Blog, 05.11.2020, https://www.scip.ch/?labs.20201105, besucht am: 14.02.2023 (zit. als VASELLA, Datenverschlüsselung in der Cloud).

VOKINGER KERSTIN NOËLLE, Gesundheitsdaten im digitalen Zeitalter, in: Jusletter 27.01.2020, https://jusletter.weblaw.ch/dam/publicationsystem/articles/jusletter/2020/1008/gesundheitsdaten-im-_bf12b7abee/Jusletter_gesundheitsdaten-im-_bf12b7abee_de.pdf, besucht am: 06.03.2023 (zit. als VOKINGER, N x).

WIDMER URSULA/BÜHLMANN LUKAS et. al., Gutachten Sekundärnutzung Gesundheitsdaten, 26. Juli 2022, https://www.interpharma.ch/wp-content/uploads/2022/10/Gutachten-Interpharma_Sekundaernutzung-Gesundheitsdaten.pdf, besucht am: 30.04.2023.

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Ausgangslage

Im Jahr 2009 war Cloud Computing etwas Neuartiges. Es wurde als Speicherung der Daten «im virtuellen Zwischenreich des Internets» oder als «Bibliothek in der Wolke» beschrieben.[1] Heutzutage ist das Cloud Computing ein zentraler Begriff und das Interesse an dieser Technologie und entsprechenden Sicherheitslösungen ist bei Unternehmen gross.[2] Auch der Bund hat im Jahr 2022 Verträge mit ausländischen Cloud-Diensten unterschrieben, um ausgewählte Daten aus den eigenen Rechenzentren auszulagern zu können.[3] Gleichzeitig häufen sich jedoch Angriffe auf Infrastrukturen von Informations-Technologien (IT) durch Cyberkriminelle, welche bspw. Datendiebstahl, Datenverschlüsselungen oder Lösegeldforderungen mit sich ziehen oder das Herunterfahren des Systems erzwingen können.[4] Clive Humby, Datenwissenschafter und Mitgründer des Karten-Treueprogramms der Supermarktkette Tesco[5], sagte 2006 am Senior Marketer's Summit der Association of National Advertisers (ANA) «Data is the new oil».[6]

Die Inkraftsetzung von neuen Datenschutzrichtlinien wie die Datenschutzgrundverordnung (DSGVO), das revidierte Übereinkommen SEV des Europarats sowie das neue Datenschutzgesetz (nDSG) sind ein Zeichen für die zunehmende Regulierung des Datenschutzes. Der technische Fortschritt in der Digitalisierung bedingt, dass personenbezogene Daten besser geschützt werden.[7] Unternehmen, welche sensible Daten verarbeiten, müssen sicherstellen, dass die Daten vor Bedrohungen geschützt sowie die Vertraulichkeit und Integrität gewährleistet werden.[8] Es stellt sich also die Frage, wie sichergestellt werden kann, dass die Datenbearbeitung auf einer Infrastruktur vertrauenswürdig, vertraulich und datenschutzkonform ist.

Das Sicherheitsdenken für das Thema Vertrauenswürdigkeit in der IT begann bereits 2003, als die Trusted Computing Group (TCG) gegründet wurde. Die TCG hatte zum Ziel, die Sicherheit von Hardware-Komponenten gegenüber Angriffen zu gewährleisten.[9] Das Kernstück von Trusted Computing ist das «Trusted Platform Module (TPM)». Der

[1] GÜNTNER, NZZ Zeitungsarchiv.
[2] HÄBERLI, Der neue Swisscom-Chef.
[3] HÄBERLI, Die umstrittenen Verträge.
[4] COVIELLO, Massiver Cyberangriff trifft die Universität Zürich.
[5] HUMBY AND DUNN, o.D.
[6] PALMER, Data is the New Oil.
[7] LEXR, DSGVO und Confidential Computing.
[8] CCC, About the Confidential Computing Consortium.
[9] ROSTEK, S. 16 ff.

TPM ist ein Chip, welcher sicherstellt, dass eine Software auf ihre Sicherheit getestet und die Vertrauenswürdigkeit einer Umgebung gewährleistet werden kann.[10]
Weitere Forschungen im Bereich einer vertrauenswürdigen und geschützten Umgebung für die Datenverarbeitung führten zum sogenannten «Trusted Executions Environment (TEE)». Dabei sollen die Daten während der Verarbeitung von keiner beteiligten Partei verändert oder gelesen werden können. Diese Technologie bildet die Grundlage für Confidential Computing, also die vertrauliche Datenbearbeitung.[11]

1.2 Ziel dieser Forschungsarbeit

Die vorliegende Forschungsarbeit beschäftigt sich mit technologischen Möglichkeiten der vertraulichen Datenbearbeitung unter der Berücksichtigung der gesetzlichen Anforderungen. Dabei werden die Eigenschaften von Trusted Computing als Ausgangslage genutzt. Anschliessend erfolgt die Überleitung zu den technologischen Möglichkeiten von Cloud Computing und Confidential Computing. In einem zweiten Schritt werden die Anforderungen, welche der Gesetzgeber an eine Datenbearbeitung stellt, betrachtet und auch aus dem Blickwinkel von Cloud-Anbietenden und deren Kundinnen und Kunden beleuchtet. Das Ziel der Forschungsarbeit ist das Aufzeigen der heutigen Herausforderungen im Bereich der Datenbearbeitung unter Berücksichtigung der gesetzlichen Anforderungen und für welche Anwendungsbeispiele Confidential Computing neue Möglichkeiten eröffnet.

1.3 Forschungsfragen

Prüfung der Datenschutzkonformität von Datenbearbeitungen durch den Einsatz von Confidential Computing unter Berücksichtigung des neuen Datenschutzgesetzes der Schweiz mit den folgenden Teilfragen:

a) Was ist der Unterschied zwischen Trusted Computing und Confidential Computing?
b) Wie muss gemäss dem neuen Datenschutzgesetz vorgegangen werden, damit eine Datenbearbeitung datenschutzkonform umgesetzt wird?
c) Welchen Beitrag kann der innovative Ansatz von Confidential Computing für den Datenschutz und insbesondere für die Datensicherheit leisten?

[10] BRANDL, S. 21.
[11] JÄGER/RIEKEN/ERNST, Herausforderung Datenschutz, S. 27 f.

1.4 Forschungsmethodik

Der Aufbau der vorliegenden Forschung richtet sich nach den in Abschnitt 1.3 erwähnten Teilfragen und der Erstellung einer Prüfung der vorgelegten Thematik: Zuerst erfolgt eine fundierte Literaturrecherche i.S.v. wissenschaftlicher Fachliteratur, relevante Materialien, öffentliche Berichte, publizierte Fachartikel und relevante Webseiten. Aufgrund der Aktualität des Themas werden in einem zweiten Schritt Experteninterviews durchgeführt. Anhand eines auf Literatur basierenden und entsprechend erstellten Leitfadens werden die Expertinnen und Experten befragt. Mittels der Auswertung und Ergebnisse der Experteninterviews und Ergebnisse aus der Literaturrecherche werden die Teilfragen a) bis c) beantwortet. Die Expertinnen und Experten werden aufgrund ihrer Funktion und beruflichen Tätigkeit selektioniert.

Da die Datenbearbeitung und nicht eine Technologie selbst als datenschutzkonform angesehen werden kann, wird in der Forschung die Veränderung der Datensicherheit i.S. einer potenziellen Risikominimierung durch den Einsatz von Confidential Computing eruiert. Dazu werden Anwendungsbeispiele genannt, welche die Nutzung exemplarisch aufzeigen sollen.

1.5 Abgrenzung

In der Forschung kommt das nDSG zur Anwendung, obwohl es zum Zeitpunkt dieser Forschungsarbeit noch nicht in Kraft ist. Sollten Gesetze und Richtlinien im Bereich des Datenschutzes (e.g. internationale Gesetze und Abkommen) für die Forschung notwendig werden, werden diese im bedarfsgerechten Masse beigezogen. Werden aufgrund der Thematik weitere gesetzliche Anforderungen relevant, werden diese erwähnt, jedoch nicht detailliert erläutert. Das nDSG wird nicht vollständig abgehandelt, sondern es werden die als relevant betrachteten Anforderungen erläutert und in der Diskussion themenfokussiert eingesetzt.

Auf technologischer Seite wird der Einsatz der erläuterten Technologie betrachtet und in den rechtlichen Kontext gesetzt. Die Kosten und der Aufwand für eine Implementierung insbesondere von Confidential Computing wird nicht thematisiert.

I THEORETISCHER TEIL: Technologie

In einem ersten Schritt werden die relevanten Technologien Trusted Computing, Cloud Computing und Confidential Computing betrachtet und deren Eigenschaften sowie Funktionalitäten im Bereich einer vertrauenswürdigen Datenbearbeitung durchleuchtet.

2 Trusted Computing

Der Begriff «Trusted Computing» wurde 1983 das erste Mal durch das amerikanische Verteidigungsministerium definiert. 1999 wurde zwischen den Mitgliedern Microsoft, International Business Machines Corporation (IBM), Hewlett-Packard und Compaq ein Konsortium namens «Trusted Computing Platform Alliance (TCPA)» gegründet mit dem Ziel, «vertrauenswürdige Computersysteme zu entwickeln». Drei Jahre nach der Gründung präsentierte Microsoft Konzepte, welche die Implementierung eines solchen Systems aufzeigte. Diese Idee stiess jedoch auf Misstrauen. Es wurde vermutet, dass die Technologie nicht die Systemkontrolle seitens des Anwenders schützt, sondern lediglich als Schutz der Digitalen Rechteverwaltung (englisch: Digital Rights Management) einen Nutzen ergeben würde. Das Thema Trusted Computing hatte im Anschluss international ein schlechtes Image. Die TCPA löste sich 2002 wieder auf. [12]

Im Jahr 2003 wurde die Trusted Computing Group (TCG) gegründet mit dem Ziel, die Sicherheit von Hardware-Komponenten gegenüber Angriffen zu gewährleisten.[13]

Inwiefern der Aufbau von Vertrauen in dieser Hinsicht eine Rolle spielt und wie die Integrität und Sicherheit der Daten mittels der Komponenten von Trusted Computing sichergestellt werden kann, wird in den folgenden Abschnitten erläutert.

2.1 Der Aufbau von Vertrauen

Heutzutage wird in fast allen Lebensbereichen bereits Software eingesetzt. In Computern, Laptops, Smartphones und auch in Autos. Fehler in einer Softwareanwendung können zu grossen Sicherheitslücken führen, welche Angreifer ausnutzen können, und dies auf immer professionellere Art und Weise. Die steigende Komplexität von IT-Infrastrukturen, mangelnde Erfahrungen in der Softwareentwicklung und der hohe Zeitdruck sind nur ein paar Gründe für die Entstehung von Softwarefehlern. Schwachstellen, welche durch einen unzureichenden Code einer Software hervorgehen, können bösartig genutzt werden,

[12] MÜLLER, S. 13.
[13] ROSTEK, S. 16 ff.

indem via Remote-Zugriff auf fremde Computer zugegriffen wird und die darauf gespeicherten Daten für andere Zwecke missbraucht werden.[14]

In dieser Hinsicht ist es somit essenziell, dass Software durch die Nutzenden als vertrauenswürdig eingestuft werden kann. Das kann bspw. über das Definieren von detaillierten Projektrichtlinien geschehen. Dabei werden jedoch Aspekte wie die Risikoeinschätzung, umfangreiches Testing, Dokumentation der Prozesse, Regelung der Zuständigkeiten etc. von Unternehmen häufig nicht korrekt umgesetzt. Die Vertrauenswürdigkeit kann auch durch Zertifizierungen aufgebaut werden, wobei die IT-Infrastruktur durch eine qualifizierte, externe Organisation auf ihre Vertrauenswürdigkeit geprüft wird. Auch Qualitätssiegel werden genutzt, damit bestätigt werden kann, dass die IT-Sicherheit einer Software den Kriterien, welche das Qualitätssiegel definiert, entspricht. Der Vertrauensaufbau und die Übernahme von Verantwortung seitens der Hersteller spielen im Bereich von IT-Infrastrukturen somit eine zentrale Rolle. Die Basis für die Schaffung von Vertrauen basiert jedoch auf dem Aufbau einer «Trusted Platform».[15]

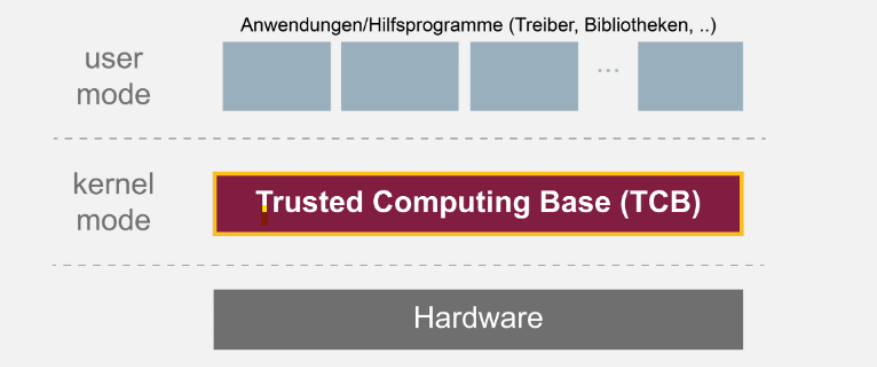
Gemäss der TCG steckt hinter dem Begriff «Trust» eine gewisse Erwartung des Verhaltens. Dieses Verhalten muss nicht zwingend positiv, resp. vertrauenswürdig sein. Damit man das Verhalten einer Plattform einschätzen kann, muss deren Identität in Erfahrung gebracht werden. Weisen eine Hardware und eine Software ein identisches Verhalten auf, sollten auch die Eigenschaften der beiden gleich sein.[16]

2.2 Der technische Aufbau

Die «Trusted Computing Base (TCB)» wird als zuverlässige Basis des Trusted Computing angesehen. Auf dieser vertrauenswürdigen Basis können weitere Bausteine implementiert werden. Wird in der TCB eine Schwachstelle aufgedeckt, kann das gesamte System missbraucht werden. Findet der Angriff ausserhalb der TCB statt, kann der Schaden aufgrund der Sicherheitsvorkehrungen eingeschränkt werden.[17] Prof. Norbert Pohlmann hat dazu eine übersichtliche Darstellung erstellt (s. Abb. 1).

[14] POHLMANN, Die Vertrauenswürdigkeit von Software, S. 655 ff.
[15] POHLMANN, Die Vertrauenswürdigkeit von Software, S. 658 ff.
[16] TCG, S. 21.
[17] POHLMANN, S. 272.

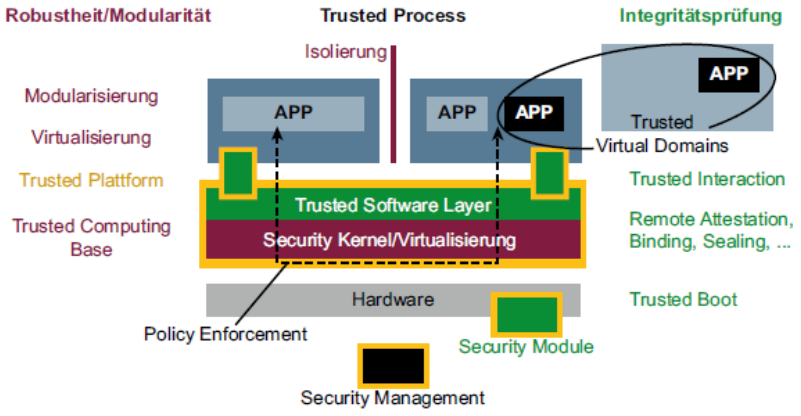
Abb. 1: Die Trusted Computing Base.



Anmerkung: POHLMANN, TCB.

Damit ein robustes IT-System gewährleistet werden kann, sind weitere Komponenten notwendig. Die Virtualisierung und Isolierung stellen Sicherheitsvorkehrungen dar, welche mögliche Schwachstellen oder bösartige Software isolieren können und stellen sicher, dass virtuelle Maschinen eigenständig funktionieren und sich nicht gegenseitig beeinflussen können. Die Modularisierung ermöglicht, individuell zu entscheiden, welche Software, basierend auf den jeweiligen Sicherheitsaspekten, in unterschiedlichen oder denselben virtuellen Maschinen laufen, wodurch ein hoher Grad an Cyber-Sicherheit sichergestellt werden kann.[18] Diese Komponenten sorgen für die Robustheit des Systems. Sie sind in der linken Hälfte der Abb. 2 zu sehen.

Abb. 2: Sicherheitsarchitektur und -prinzipien eines vertrauenswürdigen IT-Systems.



Anmerkung: POHLMANN, S. 272.

Bei Trusted Computing reicht es jedoch nicht aus, geeignete und robuste Module einzusetzen. Es muss gleichzeitig eine Prüfung der Integrität stattfinden. Nur mittels einer

[18] POHLMANN, S. 273.

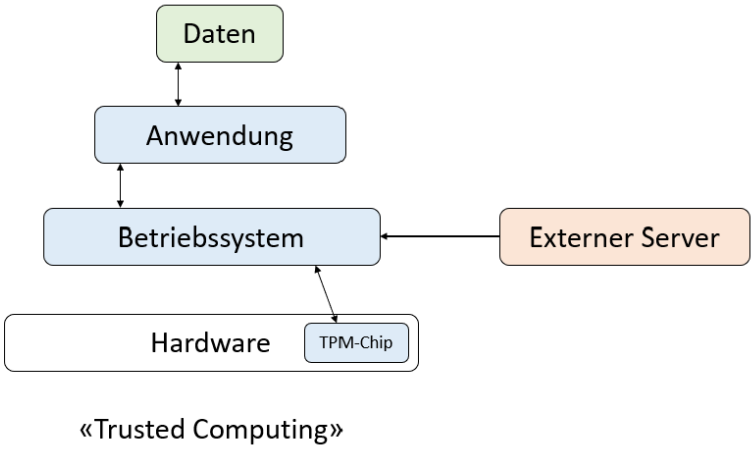
Prüfung der Integrität kann ein IT-System als vertrauenswürdig gelten. Die Integrität wird durch ein Konstrukt von Komponenten sichergestellt. Dabei bildet einen Teil davon der «Trusted Software Layer» und die daraus zusammenhängenden Sicherheitsdienste ab, welche ausgeführt werden.[19] Das Herzstück des Trusted Computings ist das «Trusted Platform Module (TPM)».[20] Deswegen wird diese Komponente im nächsten Abschnitt genauer betrachtet. Es stellt sich die Frage, weshalb sich mittels Einsatzes eines TPM die Sicherheit eines Computersystems gewährleisten lässt und wie die Daten von Nutzenden dadurch geschützt werden.

2.2.1 Eigenschaften eines Trusted Platform Module (TPM)

Das TPM, früher auch als «Fritz Chip» bekannt, welches lange Zeit eher misstrauisch betrachtet wurde, hat sich durch die zusätzlichen Sicherheitsfunktionen, welche sich durch den Einsatz eines TPM ergeben, zu einem Standard entwickelt.[21] Heutzutage wird in allen Computer standardmässig ein TPM eingebaut. Die TPM werden zudem laufend weiterentwickelt und den aktuellen Sicherheitsstandards angepasst.[22]

Das TPM wird in der Hardware eines Computers verbaut.[23] Es bildet in der Infrastruktur kein aktives Element und erhält deshalb die Anweisungen durch ein zuverlässiges Betriebssystem.[24] (s. Abb. 3).

Abb. 3: Der Aufbau von «Trusted Computing».



Anmerkung: Eigene Darstellung in Anlehnung an ROHR, S. 59; BRANDL, S. 21; SEAMON CHAN, TONG/KE XUE, Trusted Computing.

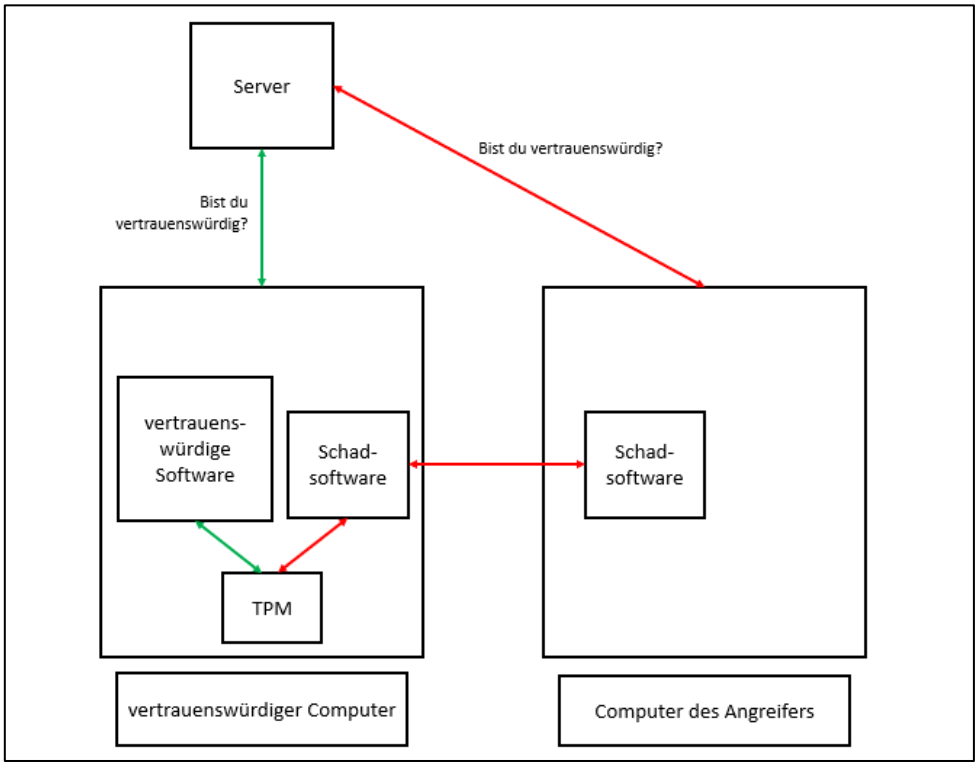
[19] POHLMANN, S. 273 f.
[20] BRANDL, S. 21.
[21] WEISS, S. 140.
[22] Intel, Trusted Platform-Modul (TPM) – Überblick.
[23] ROHR, S. 59.
[24] BRANDL, S. 21.

Anhand des TPM können kritische Daten, wie bspw. Benutzerzugangsdaten, Zertifikate und Verschlüsselungsschlüssel auf dem Computer sicher gespeichert und vor externen Angriffen geschützt werden. Zum anderen kann durch das TPM eine Authentifizierung des Computersystems und somit dessen Integrität geprüft werden. Diese Funktion wird anhand des Startvorgangs eines Computers ersichtlich, bei dem das TPM einen Verschlüsselungsschlüssel bereitstellt. Mittels dieses kryptografischen Schlüssels kann der verschlüsselte Datenträger entsperrt werden und der Computer wird hochgefahren. Findet keine gültige Validierung statt, ist ein Startvorgang des Computers unmöglich. Diese Situation kann eintreffen, wenn der Verschlüsselungsschlüssel des TPM manipuliert wurde.[25]

Zu beachten ist jedoch, dass ein TPM rein von seiner Funktion her nicht unterscheiden kann, ob eine Information vom eigenen Rechner erstellt wurde oder extern generiert wurde. Das bedeutet folglich, dass Informationen einer gutartigen Software nicht von Informationen einer bösartigen Software differenziert werden können. Das TPM kann somit von Angreifern missbraucht werden, damit diese auf einen Server Zugriff erhalten. So einfach wie es klingt, ist es aber für Angreifer nicht, sich über einen fremden Computer als vertrauenswürdiges Computersystem auszugeben.[26] Dieses Szenario wurde aus Gründen der Nachvollziehbarbarkeit in Abb. 4 grafisch dargestellt.

[25] Intel, Trusted Platform-Modul (TPM) – Überblick.
[26] SEGALL, S. 17.

Abb. 4: TPM-Missbrauchsszenario über eine Schadsoftware



Anmerkung: Eigene Darstellung in Anlehnung an Segall, S. 17.

2.3 Ziele

Eines der Ziele von Trusted Computing ist, dass anhand einer «Hardware-Based Root of Trust», einem sogenannten «Vertrauensanker» die Integrität hardwarebasiert und nicht softwarebasiert implementiert wird, was ein erhöhtes Sicherheitsniveau in der Basis der Hardware gewährleistet. Hat man diese sichere Basis erstellt, kann man mit der sogenannten «Chain of Trust», der «Vertrauenskette», die Integrität von sämtlichen Komponenten sicherstellen. Zentral ist dabei, dass alle Komponenten miteinander über vertrauenswürdige Pfade verbunden sind. Mittels erstellter Protokolle lässt sich die Vertrauenswürdigkeit der Systemhardware sicherstellen («Platform Attestation»). Dabei wird überprüft, ob die Hardware auf einer «Trusted Computing Platform» aufgebaut ist. Ein weiteres Ziel des Trusted Computing definiert sich über die eindeutige Identifizierung eines Systems und somit einer Fälschungs- und Kopiersicherheit («Platform Authentification»). Eine Fälschungs- und Kopiersicherheit kann bei einer softwarebasierten und -geschützten Identität nicht zugesichert werden. Aus diesem Grund muss die Identität sicher in der Hardware integriert werden.[27]

[27] MÜLLER, S. 16 ff.

Pohlmann vergleicht die Attestation zwischen Hardware- und Softwarekomponenten, resp. die Systemkonfiguration für einen sicheren Startvorgang eines Computers mit dem Zusammenbau eines Autos. Während der Montage muss eine Person regelmässig die Kontrolle der verbauten Automobilteile vornehmen und dabei Protokoll führen. Die Sicherheit und Echtheit des Autos können somit bewiesen werden. Wird beim Auto ein Ersatzteil angebracht, welches nicht mehr dem Original entspricht, ist das Auto im Vergleich zum Original nicht mehr vertrauenswürdig. Eine solche Überprüfung ist durch das TPM sichergestellt.[28]

Das zusätzliche Versiegeln der Dateien, welches als «Sealing» bezeichnet wird, ermöglicht den Zugriff auf die Daten ausschliesslich, wenn die Konfiguration zu Hardware und Software identisch ist. Die Daten werden dafür an die Systemkonfiguration gebunden und beim Speichervorgang signiert.[29]

Die hier aufgeführten Ziele wurden nicht abschliessend erfasst, da ein detaillierteres Ausmass der technischen Gegebenheiten sich ausserhalb des Forschungsrahmens befinden. Die nachfolgenden konkreten Anwendungsbeispiele untermalen die erläuterten Ziele[30]:

Authentifizierung eines Computersystems: Ein TPM ermöglicht die Überprüfung der Identität eines Computers und erlaubt den Datenfluss zwischen den zwei Geräten. Mit dieser Funktion können bspw. Firmen sicherstellen, dass nur unternehmensinterne Geräte eine Verbindung zum VPN-Netzwerk (engl. Virtual Private Network) herstellen können.

Datenschutz: Durch das TPM kann die Festplatte verschlüsselt werden, damit der Einsatz einer kopierten Festplatte erkannt wird und somit kein Zugriff möglich ist. Daten, welche durch ein TPM verschlüsselt sind, sind ausserhalb des Computers nutzlos. Anders verhaltet es sich jedoch mit Daten, welche entschlüsselt auf dem Computer verwendet werden. Diese werden durch das TPM nicht geschützt.

Attestierung: Ein Server überprüft anhand des TPM die Integrität des Gerätes über das Netzwerk («Remote Attestation»). Diese Funktion erlaubt die Übermittlung von sensiblen Daten an einen externen Server, bei dem die Integrität vorgängig sichergestellt wurde. Ist auf dem entfernten Computer auch noch die erwartete Software vorhanden, werden die sensiblen Daten entschlüsselt.

[28] POHLMANN, S. 123.
[29] BRANDL, S. 26.
[30] SEGALL, S. 17 ff.

2.4 Exkurs: Trustworthy Computing (TwC)

Während der Jahrtausendwende nahmen die finanziellen Schäden und Ausfälle auf kritischen Anwendungen und Systemen verursacht durch Angriffe zu. Es wurden gezielt Schwachstellen aufgedeckt und ausgenutzt. Microsoft stellte daraufhin den gesamten Konzern auf «Trustworthy Computing (TwC)» um. Alle Prozesse wurden unterbrochen und es fanden Umstrukturierungen statt, damit umfangreiche Sicherheitsmassnahmen eingeführt und umgesetzt werden konnten. Die neuen Prinzipien «Secure by Design» und «Secure by Default» stellten den Start dar zur Etablierung der Durchführung von systemischen Tests, repetitiven Tests der programmierten Codes und es wurden kompetente Verantwortliche ernannt, welche die einzelnen Entwicklerteams in Sachen Sicherheit hin zu TwC i.S.v. «Security, Privacy, Reliability» trieben. In diesem Kontext wurde viel Kommunikation durch Aufklärungsinitiativen, Schulungen und Sensibilisierung im Umgang mit Informationstechnologien unternommen.[31]

Microsoft wollte Verantwortung übernehmen, Vertrauen schaffen und sich gegenüber den Anwendern als verlässliches Unternehmen positionieren. Aus diesem Grund war es Microsoft ein Anliegen, dass der Anwender darüber informiert wird, wie die privaten Daten angewendet werden. Zudem soll dem Anwender der Zugang zu den Daten auch für eine allfällige Mutation sichergestellt sein. Aus den erwähnten Handlungsfelder ist ersichtlich, dass die Einführung von TwC die Weiterentwicklung der Sicherheitsmassahmen in der IT-Sicherheit vorantrieb, was gleichzeitig auch eine Sensibilisierung der Privatsphäre im Internet nach sich zog.[32]

2.5 Vergleich Trusted Computing und Trustworthy Computing (TwC)

Vergleicht man Trusted Computing und TwC sticht heraus, dass Trusted Computing den Schwerpunkt auf die Hardware-basierte Sicherheit legt und somit in diesem Bereich technische Massnahmen erhebt. Im Gegensatz dazu fokussiert sich TwC auf vertrauensbasierte und verlässliche Software und Betriebssysteme. Dabei liegt die Orientierung tendenziell eher auf dem Datenschutz zu Gunsten des Anwenders und nicht, wie bei Trusted Computing, auf der Technologie, resp. auf der Sicherstellung eines beständigen und sicheren Betriebssystems. Übergeordnet unterstützen jedoch beide Ansätze die Sicherheitsziele «Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit».[33]

[31] ROHR, S. 58.
[32] HALBHEER, S. 126.
[33] ROHR, S. 58 f.

2.6 Zwischenfazit Trusted Computing

Trusted Computing gewährleistet als Hardware-basierte Technologie die sichere Speicherung von Benutzerdaten, Zertifikaten und Schlüsselmaterial[34] und bietet die Überprüfung der Integrität eines Computersystems (durch «Attestation»)[35]. Der Zugriff auf Daten wird aufgrund der «Sealing»-Funktion nur ermöglicht, wenn Hard- und Software erfolgreich validiert werden konnte. Der Hauptfokus liegt somit, auf der Gewährleistung eines sicheren Betriebssystems und sicheren Datenspeicherung.[36]

Die Digitalisierung ermöglicht Nutzerinnen und Nutzer eine zunehmende Vernetzung. Die Vernetzung und die Möglichkeiten von Cloud Computing werden im nächsten Kapitel dargelegt.

[34] Vgl. Kap. 2.2.1
[35] Vgl. Kap. 2.3
[36] Vgl. Kap. 2.3

3 Cloud Computing

Die technologischen Fortschritte in den Bereichen der Mobilität und der Virtualisierung von Daten ermöglichen es Nutzerinnen und Nutzer sowie Anbietenden, Werke niederschwellig in der sogenannten «Cloud» zu speichern, diese Werke darin zu mutieren sowie weitere Bearbeitungsschritte auszuführen. In diesem Bereich besteht ein wachsender Markt.[37]

Die fortschreitende digitale Vernetzung hat dazu geführt, dass die meisten Geräte, welche durch Endkonsumenten genutzt werden, über eine Anbindung an eine Cloud verfügen. Eine Fitness-Armbanduhr speichert gesundheitliche Daten wie Bewegungsmuster, Schlafgewohnheiten und weitere persönliche sowie auch medizinische Daten in einer Cloud. Werden die Daten unrechtmässig bearbeitet, hat dieser Umstand einen Einfluss auf die Selbstbestimmung einer Nutzerin oder eines Nutzers.[38]

In den folgenden Abschnitten werden die technischen Gegebenheiten der Verschlüsselung von Daten und anschliessend die unterschiedlichen Cloud-Dienste und deren Fähigkeiten erläutert.

3.1 Definition

Cloud Computing (Cloud) ist aufgrund der Komplexität schwierig, einheitlich zu definieren. Als Cloud kann eine Infrastruktur verstanden werden, welche über ein Netzwerk zugänglich gemacht wird. Darin werden den Nutzerinnen und Nutzern Dienstleistungen wie bspw. Software oder Speicherplatz zur Verfügung gestellt.[39]

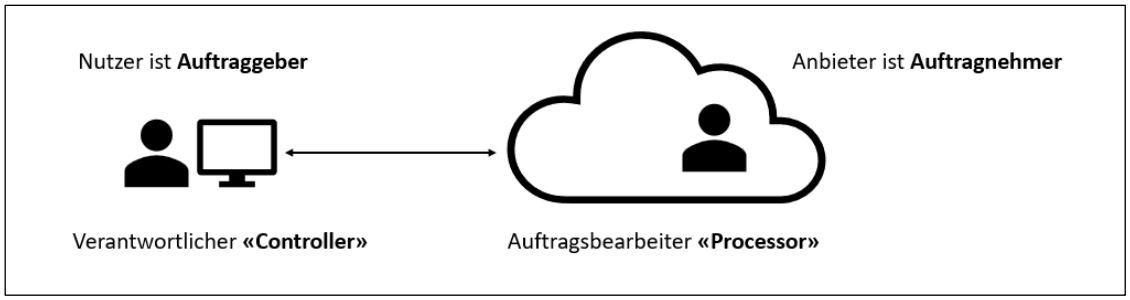
Gerne wird in der Literatur auch die Definition des «National Institute of Standards and Technology» (NIST) zitiert. Dabei wird die Cloud als Nutzer-freundliches Modell für den Netzzugang zu einem gemeinsamen Pool definiert. Darin können mittels minimalem Verwaltungsaufwand und minimaler Interaktion zwischen dem Anbieter und dem Nutzer Ressourcen wie Server, Speicher, Anwendungen und weitere Dienstleistungen, bereitgestellt werden.[40]

Vereinfacht erklärt handelt es sich bei der Cloud um eine Dienstleistung um die Auslagerung der Infrastruktur zu einem Cloud-Anbieter, welcher, abhängig von der durch den Auftraggebenden gefragten Dienstleistung, Softwareanwendungen, Speicherplatz und Serverleistung zur Verfügung stellt und somit den Prozess für die Nutzenden

[37] BERANEK/DE LA CRUZ BÖHRINGER, S. 663.
[38] HERFERT/LANGE /SPYCHALSKI, S. 128.
[39] BLONSKI, S. 65.
[40] NIST, The NIST Definition of Cloud Computing, S. 2.

vereinfacht.[41] Der Cloud-Anbieter agiert gegenüber Cloud-Nutzenden sozusagen als Auftragnehmer (s. Abb. 5).[42]

Abb. 5: Auftragsverhältnis zwischen Cloud-Anbietenden und Cloud-Nutzenden



Anmerkung: Eigene Darstellung in Anlehnung an JÄGER/RIEKEN/ERNST, S. 9.

In diesem Auftragsverhältnis gibt es unterschiedliche Dienstleistungsmodelle, welche auch Einfluss auf die Verantwortung, Kontrolle und den Schutz der Daten haben.

3.2 Servicemodelle

Infrastructure as a Service (IaaS)

Die Nutzerin und der Nutzer der Cloud können Daten und individuelle Anwendungen auf einem Server, welcher sich in der Cloud befindet, speichern und betreiben. Dieser Server wird durch den Cloud-Anbieter zur Verfügung gestellt und so weit unterhalten, damit die Netzfunktion und alle weiteren Funktionalitäten gewährt sind.[43]

Platform as a Service (PaaS)

Der Cloud-Anbieter ist in der Entwickler-Rolle und stellt Anwendungen in der Cloud zur Verfügung.[44]

Der Cloud-Anbieter hat stets die Kontrolle über die Cloud-Infrastruktur (Netzwerk, Server, Betriebssystem oder Speicher). Die Nutzenden hingegen verfügt über die Kontrolle der installierten Anwendungen innerhalb der Infrastruktur.[45]

[41] HERFERT/LANGE/SPYCHALSKI, S. 128.
[42] JÄGER/RIEKEN/ERNST, S. 9.
[43] EDÖB, Erläuterungen zu Cloud Computing.
[44] EDÖB, Erläuterungen zu Cloud Computing.
[45] NIST, The NIST Definition of Cloud Computing, S. 2 f.

Software as a Service (SaaS)

Die Nutzenden der Cloud können keine individuellen Anwendungen oder Daten mehr bewirtschaften. Die Cloud bildet ein Konstrukt für die Datenbearbeitung. Es handelt sich somit nur noch um ein Konsumgut.[46]

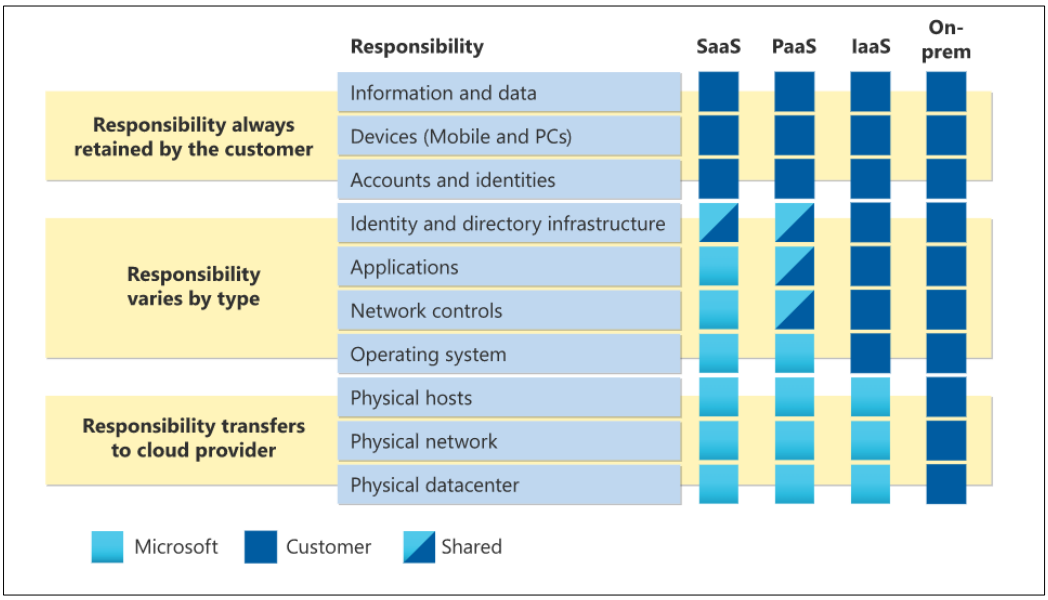
Die Entwicklungen in diesem Bereich der Cloud-basierten Services zeigen, dass auch zunehmend bedarfsgerechte Lösungen durch die Unternehmen beansprucht werden. Dieser Umstand löst Schnittstellen zwischen den unterschiedlichen Services aus. Der flexible und massgeschneiderte Einsatz von diversen Dienstleistungen lässt eine Entwicklung hin zu «Everything as a Service» deuten. Dabei spielen im Kontext der digitalen Bedrohungen, Sicherheits-Dienstleistungen, welche Nutzerinnen und Nutzer über die Cloud beziehen können, eine zentrale Rolle.[47]

Diese drei erläuterten Servicemodelle können als «Private Cloud», «Public Cloud» oder «Hybrid Cloud» genutzt werden. Eine «Private Cloud» wird für den internen Gebrauch eines Unternehmens gebaut. Dagegen bietet bei einer «Public Cloud» ein externer Anbieter seine Infrastruktur an, welche auch andere Unternehmen zur selben Zeit nutzen. Die «Hybrid Cloud» stellt eine Kombination der ersten zwei Modelle dar. Welche Art der Cloud ein Unternehmen wählt, ist meistens abhängig von der Höhe der Investitionsmöglichkeiten. Der Aufbau einer Privaten Infrastruktur ist kostspielig, weshalb die Wahl oftmals auf letztere zwei Servicemodelle fällt.[48]

Wie sich die Verantwortungen in den unterschiedlichen Dienstleistungspaketen aufteilt zwischen Cloud-Anbieter und den Nutzenden, hat Microsoft in einer Übersicht zusammengestellt (s. Abb. 6).

[46] EDÖB, Erläuterungen zu Cloud Computing.
[47] VISCARDI, Sicher in der Cloud - durch die Cloud?
[48] KÜDERLI, Im Fokus: Neue Geschäftsmodelle, Die wahren Vorteile der Cloud und die Nachteile

Abb. 6: Das Modell der «Shared Responsibility» in der Cloud von Microsoft.



Anmerkung: Microsoft, Shared Responsibility.

In der Abb. 6 ist ersichtlich, dass die Daten unabhängig des gewählten Services, in der Verantwortung der Nutzerin oder des Nutzers bleiben und die technische Infrastruktur entsprechend dem gewählten Service in der Verantwortung des Cloud-Anbieters ist. Ein zentrales Entscheidungskriterium für die Nutzenden stellt sich in der Frage, wie die Daten geschützt werden.

3.3 Technischer Schutz der Daten

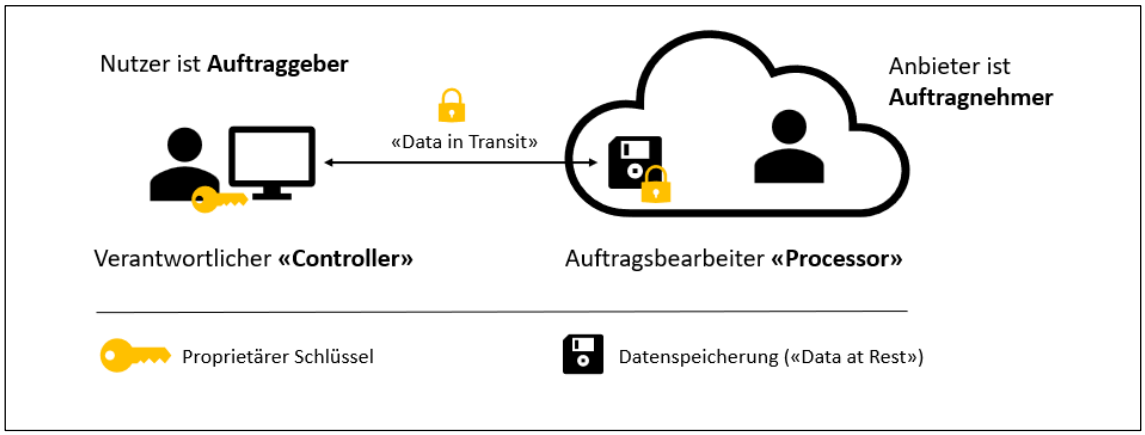
Beim Thema Auslagerung an einen Cloud-Anbieter ist der Schutz der Daten der Nutzerin oder des Nutzers von zentraler Bedeutung. Die Daten müssen während des Transfers zwischen den Nutzenden und Cloud-Anbieter, während der Speicherung sowie während der Verarbeitung durch den Cloud-Anbieter geschützt sein.[49] Die Datenübermittlung, die Datenspeicherung und die Datenbearbeitung sind in der Literatur häufig unter den folgenden Begriffen anzutreffen: «Data in Motion» oder «Data in Transit», «Data at Rest» und «Data in Use».[50] Diese drei Zustände müssen im Kontext der Verschlüsselung differenziert betrachtet werden.

Bei der Datenübermittlung werden die Daten über ein privates oder ein öffentliches Netzwerk von einem Gerät auf ein anderes Gerät übertagen. Während der Übermittlung sind die Daten verschlüsselt, was die Daten vor Abhören und Mitlesen schützt. Bei einer Datenspeicherung befinden sich die Daten abgespeichert und inaktiv auf einem Gerät. Die

[49] HERFERT/LANGE /SPYCHALSKI, S. 128.
[50] VASELLA, Datenverschlüsselung in der Cloud.

Daten sind in diesem Zustand verschlüsselt, was die Daten vor unerlaubter Einsicht und Datendiebstahl schützt.[51] Es liegen somit Technologien für den verschlüsselten Datentransfer sowie Datenspeicherungen vor (s. Abb. 7).

Abb. 7: Verschlüsselung bei einer Datenübermittlung und Datenspeicherung («Data in Transit» und «Data at Rest»).



Anmerkung: Eigene Darstellung in Anlehnung an JÄGER/RIEKEN/ERNST, S. 9; Kaspersky, Verschlüsselung bei der Speicherung vs. Verschlüsselung bei der Übertragung.

Eine Datenbearbeitung bedingt, dass die Daten entschlüsselt vorliegen, was eine grössere Angriffsfläche für eine Kompromittierung bietet.[52] Was das für die Verschlüsselungen für Datenbearbeitungen in einer Cloud bedeutet, wird im folgenden Abschnitt anhand eines Beispiels gezeigt.

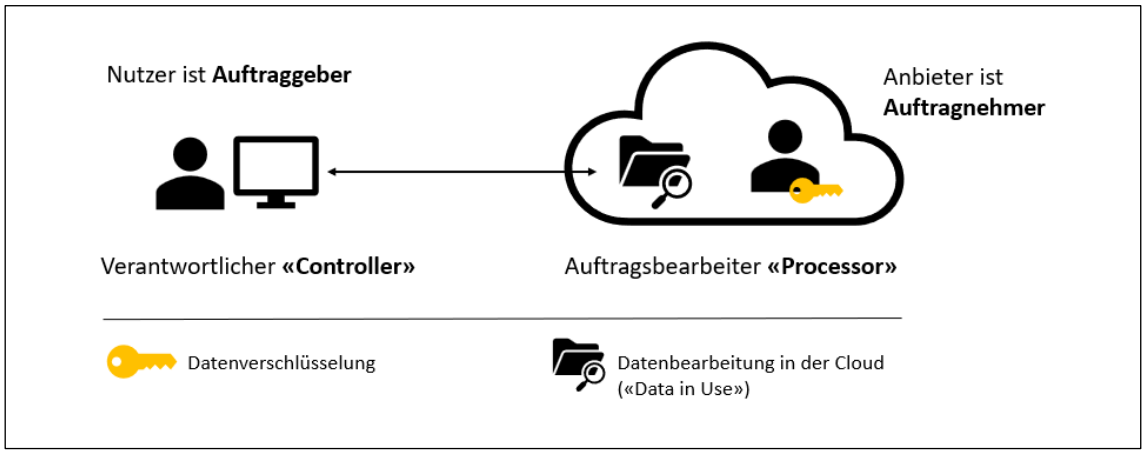
Microsoft bietet mit Office 365 Cloud-basierte Applikationen an. Damit die Daten vertrauenswürdig geschützt werden, wird der Zustand der Daten («Data in Transit», «Data at Rest» und «Data in Use»[53]) bei der Wahl der Verschlüsselungstechnik entsprechend berücksichtigt. Gespeicherte Daten werden mit Technologien Laufwerkverschlüsselungen, Speicherverschlüsselungen, Schlüssel-Managementsystemen und Microsoft 365-Dienstverschlüsselungen geschützt. Bei einer Datenübertragung werden die Daten durch die Verwendung von Protokollen, welche zwischen den Rechenzentren von Microsoft und dem Gerät der Nutzerin oder des Nutzers erstellt werden, geschützt.[54] Da die Kundendaten durch Cloud-Anbieter in Rechenzentren verschlüsselt und entschlüsselt werden, liegt der generierte Schlüssel für die Entschlüsselung der Daten auch beim Cloud-

[51] Kaspersky, Verschlüsselung bei der Speicherung vs. Verschlüsselung bei der Übertragung.
[52] HERFERT/LANGE/SPYCHALSKI, S. 130.
[53] vgl. Kap. 3.3
[54] Microsoft, Verschlüsselung in der Cloud.

Anbieter vor, was bedeutet, dass der Cloud-Anbieter Zugriff auf die Klartexte der Daten hat, was ein Nachteil für den Schutz der Daten nach sich zieht.[55]

In diesem Zusammenhang muss man die unterschiedlichen Dienstleistungs-Pakete einer Cloud unterscheiden. Bei der Nutzung eines reinen Cloud-Speicherdienstes ist es technisch möglich, die Daten nutzerseitig zu verschlüsseln. Obwohl die Anforderungen zu einer nutzerseitigen Verschlüsselung durch verfügbare «Programmbibliotheken» niedrig wären, wird diese Art der Verschlüsselung verhältnismässig gering genutzt. Begründet wird dieser Umstand einerseits durch die fehlende Nachfrage seitens der Nutzenden und andererseits durch die Vorteile, welche sich aus dem vorhandenen Zugriff seitens der Cloud-Anbieter ergeben,[56] denn eine Cloudanwendung kann Daten, welche verschlüsselt sind, nicht bearbeiten.[57] Sobald der Cloud-Anbieter Zugriff auf den Schlüssel hat, was durch die Dienstleistung einer serverseitigen Verschlüsselung gegeben ist, ist der Zugriff auf Klartexte möglich (s. Abb. 8).[58]

Abb. 8: Datenverschlüsselung und Datenbearbeitung in der Cloud



Anmerkung: Eigene Darstellung in Anlehnung an JÄGER/RIEKEN/ERNST, S. 9; VASELLA, Datenverschlüsselung in der Cloud.

Es stellt sich somit die Frage, mit welchen Ansätzen Daten in Bearbeitung vor Zugriffen geschützt werden können.

[55] HERFERT/LANGE/SPYCHALSKI, S. 130.
[56] HERFERT/LANGE/SPYCHALSKI, S. 128 f.
[57] VASELLA, Datenverschlüsselung in der Cloud.
[58] HERFERT/LANGE /SPYCHALSKI, S. 128 f.

3.4 Nutzen, Chancen und Herausforderung einer Cloud

Ein Unternehmen kann durch die Auslagerung der Hardware- und Software-Infrastruktur hohe Investitionen einsparen, da lokale Infrastruktur nicht mehr notwendig ist und auch der Unterhalt der Server (bspw. Betriebs- und Wartungsarbeiten) in der Verantwortung des Cloud-Anbieters liegt. Die Flexibilität in der Nutzung sorgt zudem zu einer Steigerung der Effizienz, da der Einsatz individuell ausgestaltet und skaliert werden kann. Die Kostenreduktion der Cloud-Lösungen eröffnet auch kleineren Unternehmen die Nutzung von professionellen IT-Lösungen, welche vorher nur mit hohen Investitionen umsetzbar waren. Kleinere- und mittlere Unternehmen profitieren insofern von einem Cloud-Anbieter, da der Anbieter über Backup-Lösungen zur Datensicherheit verfügt, erweitertes Zugriffsmanagement und eine verbrauchsabhängige Kostenabrechnung erlaubt, was vordergründig auch im Bereich von Lizenzmodellen für Grossunternehmen interessant ist. Dennoch muss bei einer Auslagerung von Daten beachtet werden, dass die Kontrolle zu einem gewissen Masse abgegeben wird. Die Sicherheit der Daten hängt von der Sicherheit der externen Infrastruktur ab. Zu berücksichtigen ist auch der Standort der ausgelagerten Daten. Aufgrund des Begriffs «Cloud», übersetzt als «Wolke» können die Nutzenden nur schwer einschätzen, wo sich die Daten befinden. Grosse Cloud-Anbieter besitzen unterschiedliche Datacenter, welche sich auf der ganzen Welt verteilen.[59] Der niederschwellige Zugriff auf die Daten hat ökonomisch hohes Potenzial. Nebst der Datensicherheit müssen jedoch auch bspw. die Aspekte des Zugriffs bei einem Systemausfall, Kündigung oder Konkurs sowie die Kosten der Dienstleistung vertraglich abgesichert werden. Eine vollumfängliche Prüfung des Anbieters und seinen Fähigkeiten müssen vorher geklärt und mit den internen sowie auch rechtlichen Anforderungen abgeglichen werden.[60]

Im Kontext der grenzüberschreitenden Bekanntgabe von Daten sind die Richtlinien des Schweizer Datenschutzgesetzes zu berücksichtigen, was in Kap. 5.10 der vorliegenden Arbeit erfolgt.

Gemäss einem Interview mit Chief Security Advisor Roger Halbheer ist hinsichtlich der Cloud-Nutzung zu beachten ist, dass auf technischer und emotionaler Ebene eine Diskussion geführt wird. Man müsse jedoch keinen grossen Unterschied zwischen der physischen und digitalen Sicherheit machen. Zentral sei, wie man mit den Risiken umgeht. Dabei solle ein vertretbarer Mittelweg zwischen der Sicherheit und der

[59] SCHLÜTER/TEUFEL, S. 6-9.
[60] KÜDERLI, Im Fokus: Neue Geschäftsmodelle, Die wahren Vorteile der Cloud und die Nachteile.

Benutzerfreundlichkeit angestrebt werden. Ob sich ein Unternehmen für die Auslagerung der Daten auf eine Cloud entscheidet, basiere auf den folgenden drei Bereichen:

- Welche Möglichkeiten sind für die technische Ausgestaltung des Datenschutzes und der Datensicherheit vorhanden und wie werden sie umgesetzt?
- Welche regulatorischen Anforderungen müssen für eine Migration in eine Cloud erfüllt sein?
- Welche «emotionalen» Konsequenzen stellt eine Migration in die Cloud für den Kunden dar?

Bei der letzteren Fragestellung steht meist der Kontrollverlust der Daten seitens des Kunden im Raum, welcher eine Auslagerung in die Cloud nach sich zieht. Bei der Evaluation der Risiken sei es jedoch essenziell, die technischen Prozesse und rechtlichen Anforderungen zu verstehen und diese klar von den emotionalen Fragen anzugrenzen. Nur so könnten die Risiken richtig evaluiert werden.[61]

3.5 Aktualitätsbezug: Public Cloud des Bundes

Am 15. Februar 2023 gab der Bundesrat bekannt, dass die bestehenden Microsoft Anwendungen in der Bundesverwaltung nicht mehr zeitgemäss sind und durch eine neue Anwendung ersetzt werden müssen. Es wurde entschieden, die Anwendung Microsoft 365, welche auf einer Public Cloud aufbaut zu implementieren. Obwohl die Abhängigkeit zu Microsoft mit diesem Schritt grösser wird, wird ein Wechsel des Anbieters oder des Produkts zurzeit nicht in Erwägung gezogen, da der Aufwand als zu gross und risikobehaftet eingestuft wird. Der Transfer in die Cloud hängt mit hohen Schutzmassnahmen zusammen. Es dürfen durch die Nutzerinnen und Nutzer keine besonders schützenswerten oder vertrauliche Daten in die Cloud gespeichert werden. Der EDÖB nahm Stellung zu den Entwürfen der Analyse der Rechtsgrundlagen und zu den Informationssicherheits- und Datenschutz-Konzepten. Der Beauftragte kam dabei zum Schluss, dass die Angemessenheit der bestehenden Rechtsgrundlagen des US-Konzerns für die Datenbearbeitung in der Cloud umfassend geprüft werden muss. Hinsichtlich der besonders schützenswerten Daten verlangt der EDÖB, dass eine Datenschutz-Folgenabschätzung erstellt wird, damit die durch eine Auslagerung entstehenden Risiken aufgezeigt werden können. Nicht ausser Acht zu lassen ist zudem der Fakt, dass das FBI auf Daten, welche in der

[61] Microsoft Switzerland, Interview mit Security-Spezialist Roger Halbheer.

Cloud gespeichert sind, Zugriff haben könnte. Aufgrund der Bedenken fordert der EDÖB den Bundesrat auf, dass weitergehend Alternativen gesucht werden sollen.[62]

3.6 Zwischenfazit Cloud Computing

Die Cloud ermöglicht die Auslagerung von Dienstleistungen im Bereich der Datenbearbeitung.[63] Dabei werden unterschiedliche Dienstleistungen angeboten, welche von der Datenspeicherung (Infrastructure as a Service) bis hin zur vollständigen Nutzung der Anwendungen, welche eine Cloud für die Datenbearbeitung anzubieten hat (Software as a Service). Unabhängig vom Servicemodell bleibt der Verantwortliche, der sogenannte «Controller» immer in der Verantwortung der Daten, wobei der Auftragsbearbeiter, der sogenannte «Processor», verantwortlich ist für die Infrastruktur.[64]

Erwähnt wurden die drei Aggregatszustände der Daten. Werden Daten übermittelt («Data in Transit») oder gespeichert («Data at Rest»), werden sie durch bestehende Verschlüsselungsmechanismen bereits angemessen geschützt. Anders verhält es sich, wenn Daten in der Cloud bearbeitet werden («Data in Use»). Diese Daten liegen unverschlüsselt vor, was bedeutet, dass der Anbieter Zugriff darauf erhält.[65] Nebst einer flexiblen und niederschwelligen Nutzung muss ein Unternehmen sich jedoch bewusst sein, dass bei einer Auslagerung von Daten ein gewisses Mass an Kontrolle abgegeben wird. Deshalb ist eine sorgfältige Prüfung eines Anbieters vorab durchzuführen und mit den internen Anforderungen des Verantwortlichen sowie rechtlichen Anforderungen zu vergleichen.[66]

Das Problem mit der Verschlüsselung von Daten, welche sich in Bearbeitung befinden, ist jedoch noch ungelöst. Mit Confidential Computing folgt im nächsten Kapital eine Technologie, welche Lösungen hinsichtlich dieser Problemstellung beisteuert.

[62] EDÖB, Bundesverwaltung führt Public Cloud gestützte Anwendung Microsoft 365 ein.
[63] Vgl. Kap. 3.1
[64] Vgl. Kap. 3.2
[65] Vgl. Kap. 3.3
[66] Vgl. Kap. 3.4.

4 Confidential Computing

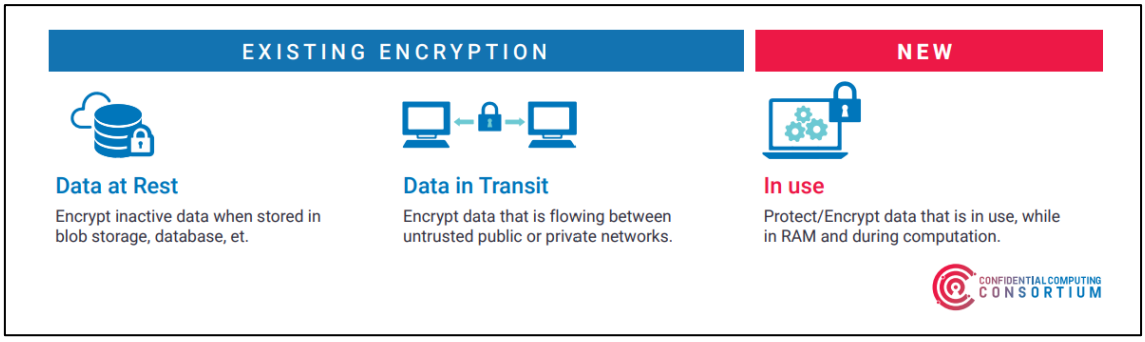
In Kap. 2 wurde mit Trusted Computing eine Technologie vorgestellt, welche technisch sichere Prozesse innerhalb der Hardware und des Betriebssystems sowie die Manipulationssicherheit der Daten gewährleistet. Dabei wurde ersichtlich, dass das TPM eine zentrale Schnittstelle für die Integrität einer Plattform und der Daten darstellt. Was die Funktionalitäten des TPM jedoch nicht bieten können, ist eine abgrenzbare geschützte Ausführungsumgebung, welche für eine Datenbearbeitung genutzt werden kann.[67] Diese Anforderung bekommt mit der im Kap. 3 aufgezeigten Cloud Computing und der zunehmenden Form der Speicherung und Bearbeitung von Daten in der Cloud einen neuen Stellenwert. Daten zu sammeln, unterliegt einem grossen Wachstum. Aufgrund der vielen gesammelten Daten werden die Datensätze fortan immer grösser.[68]

Die zunehmende Nutzung von Cloud-Diensten[69] führt dazu, dass bestehende Massnahmen, welche den Datentransfer und die Datenspeicherung schützen, für Anwendungsfälle im Bereich der Bearbeitung von sensiblen Daten, nicht mehr ausreichen. Confidential Computing ist eine hardware-basierte Technologie, welche einen Lösungsansatz für dieses Problem zu bieten hat.[70]

4.1 Vertrauen schaffen durch Technik

Daten, welche sich in Bearbeitung befinden, werden immer häufiger zur Zielscheibe von Angriffen. Confidential Computing hat zum Ziel, die unverschlüsselten Daten zu schützen, während sie sich in Bearbeitung befinden.[71] (s. Abb. 9)

Abb. 9: Bestehende und neue Verschlüsselung von Daten

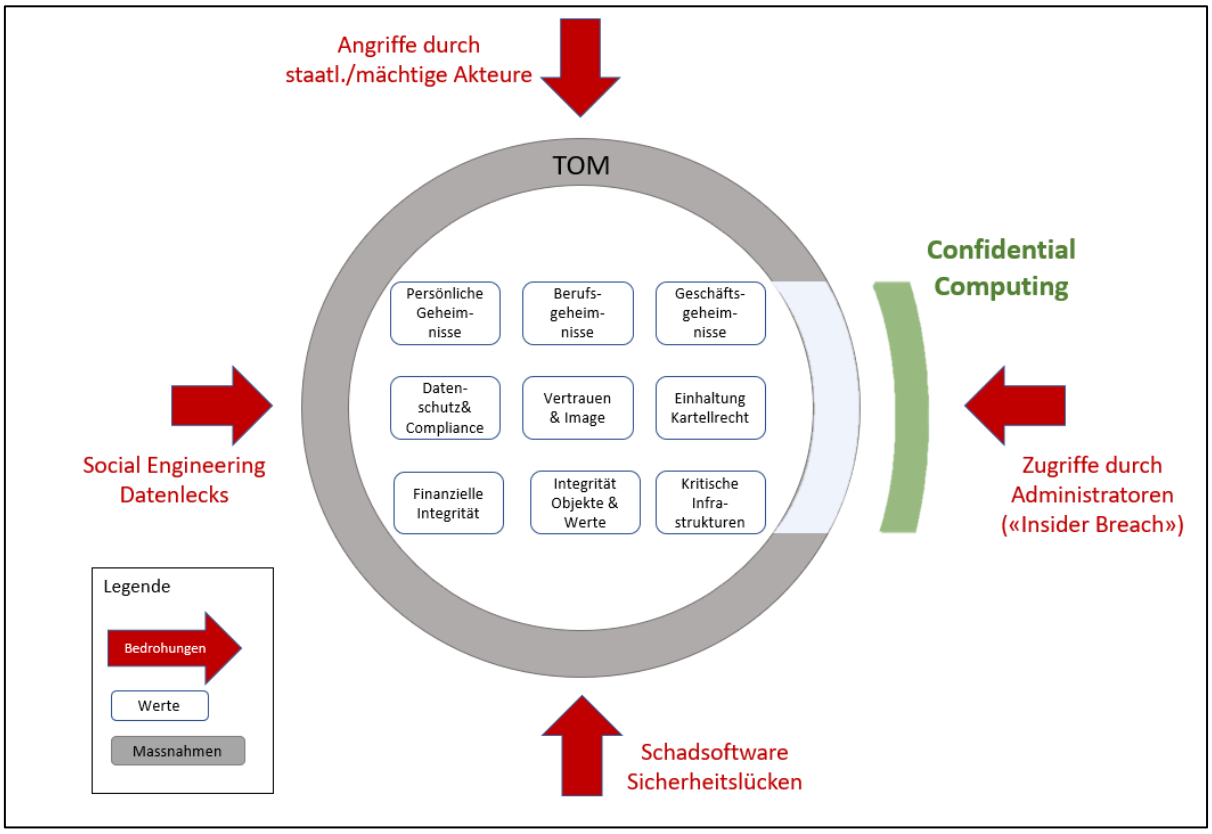


Anmerkung: CCC, Hardware-Based Trusted Execution for Applications and Data, S. 3.

[67] ACHEMLAL/BOUABDALLAH/SABT, S. 57.
[68] Microsoft Switzerland, Wie Confidential Computing Schweizer Unternehmen zu mehr Datenschutz und Sicherheit verhilft.
[69] Vgl. Kap. 3
[70] CCC, Hardware-Based Trusted Execution for Applications and Data, S. 4.
[71] CCC, Hardware-Based Trusted Execution for Applications and Data, S. 3.

In der Abb. 10 ist ersichtlich, welche Informationen (blaue Kästchen) durch Confidential Computing geschützt werden. Der graue Kreis bildet alle technischen und organisatorischen Massnahmen (TOM) ab, welche sicherstellen, dass die Bedrohungen (rote Pfeile) abgewehrt werden. In der Grafik ist ersichtlich, dass der Schutz gegenüber Zugriffen seitens der Administratoren durch herkömmliche technische und organisatorische Massnahmen ungenügend geschlossen ist. Confidential Computing kann diesen Kreis mittels einer technischen Schutzmassnahme schliessen.[72]

Abb. 10: Confidential Computing im Kontext der technischen und organisatorischen Massnahmen



Anmerkung: Eigene Darstellung in Anlehnung an JÄGER et al., Wie viel Sicherheit ist genug?, S. 178 f.

4.2 Technische Umsetzung

Confidential Computing hat folgende Eigenschaften, welche die Sicherheit der Daten gewährleisten:

«Data Clean-Up Areas»: Bei «Data Clean-Up Areas (DCUA)» handelt es sich um separierte Bereiche eines Rechenzentrums, welche bei einem fremden Zugriff die sofortige

[72] JÄGER et al., Wie viel Sicherheit ist genug? S. 178 f.

Löschung der bearbeiteten und somit unverschlüsselten Daten, resp. deren Verschiebung in einen anderen DCUA vornehmen.[73]

Schlüsselvergabe: Bei Confidential Computing werden die Schlüssel für jede Sitzung spezifisch generiert oder innerhalb der isolierten Struktur erzeugt, ohne, dass sie das Netzwerk der DCUAs verlassen. Das bedeutet, dass keine beteiligte Partei Zugriff auf den Schlüssel hat.[74]

Attestierung: Die Attestierung bestätigt die Vertrauenswürdigkeit der geschützten Umgebung. Eine erfolgreiche Überprüfung bestätigt die Richtigkeit der Daten und die Nutzung des korrekten Codes für die Bearbeitung der Daten.[75] In dieser besonders geschützten Umgebung, in der die Daten bearbeitet werden, sollen weder die Administratoren der Software noch die Betreibenden des Rechenzentrums Zugriff auf die ausgeführte Software oder auf die darin bearbeiteten Daten haben.[76]

In der Kürze lässt sich festhalten, dass es sich bei Confidential Computing um eine Technologie handelt, welche Daten während der Bearbeitung schützt, in dem die Berechnungen auf einer zertifizierten und vertrauenswürdigen Ausführungsumgebung, welche sich auf der Hardware befindet, gemacht werden.[77] Die Basis dieser Hardware, dieses sogenannte «Trusted Execution Environment (TEE)» wird im folgenden Kapitel erklärt.

4.3 Trusted Execution Environment (TEE)

Um den Nutzen eines TEE zu verstehen, muss zuerst der Kontext erläutert werden. Damit Infrastruktur und Software von Computern geschützt sind, müssen zahlreiche Codes programmiert werden. Dafür werden unterschiedliche Softwarebibliotheken und Betriebssystemdienste genutzt. Da für die Programmierung zusätzliche Komponenten wie bspw. Software und Treiber benötigt werden, entstehen zusätzliche Abhängigkeiten, bei denen der Sicherheitsstandard zu überprüfen ist. Die Endnutzerin oder der Endnutzer haben auf diese Abhängigkeiten keinen Einfluss und müssen dem Betriebssystem und der bereitgestellten Cloud Computing-Software vertrauen. Die Programmierung einer Software und die stets wachsenden Komponenten bergen jedoch die Gefahr für Schwachstellen. Da

[73] JÄGER et al., Grundprinzip der Sealed Cloud, S. 34 f.
[74] JÄGER et al., Grundprinzip der Sealed Cloud, S. 35 f.
[75] POHLMANN, Confidential Computing, Attestation bei SGX.
[76] JÄGER/RIEKEN/ERNST, S. 28.
[77] CCC, A Technical Analysis of Confidential Computing, S. 5.

setzt die Technologie des TEE ein, indem sie ermöglicht, die Menge an Codes und Komponenten zu verringern. Eine der Herausforderungen beim Cloud Computing ist das gemeinsame Nutzen derselben Hardware. Dieses Problem wurde bereits mit einer Trennung von Softwarelösungen und separierten Programmen im Betriebssystem grundlegend gelöst. Mit der Isolierung von Daten kann man jedoch noch einen Schritt weiter gehen, indem man gewisse Codes und Daten, welche zur Ausführung einen höheren Sicherheitsstandard benötigen, vom Rest des Betriebssystems isoliert.[78]

Ein TEE stellt eine solche isolierte geschützte Enklave dar, welche durch einen Systemprozessor (CPU) gesichert wird. Verschlüsselte Informationen, Authentifizierungen sowie geistiges Eigentum können im TEE sicher gespeichert sowie bearbeitet werden. Diese Funktion ermöglicht somit eine Bearbeitung innerhalb der Enklave, ohne die Daten vorher auslesen zu müssen.[79]

Das Confidential Computing Consortium (CCC) ist eine Gemeinschaft aus Hard- und Softwareproduzentinnen und- produzenten, Entwicklerinnen und Entwickler sowie Cloud-Anbietenden. Das CCC arbeitet mit Behörden zusammen und führt Kollaborationen mit Unternehmen, damit eine Sensibilisierung stattfindet im Bereich der sicheren Verschlüsselung von Datenbearbeitungen.[80]

Folgende Sicherheitsansprüche hat das CCC an ein TEE gestellt[81]:

- Datenverschlüsselung («Data Confidentiality»)
- Datenintegrität («Data Integrity»)
- Code-Integrität («Code Integrity»)

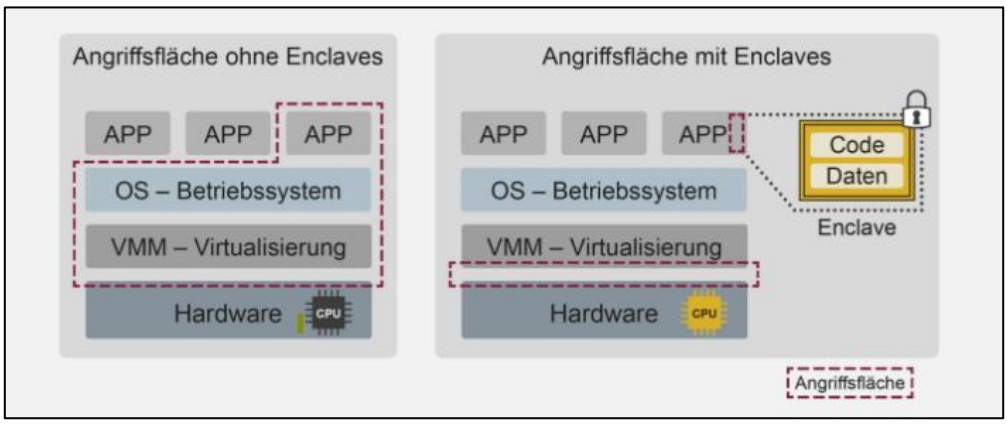
Basierend auf diesen drei Begriffen ist es keiner unbefugten Partei möglich, Daten, welche sich in Bearbeitung befinden, einzusehen, Daten oder Codes zu verändern oder zu löschen.[82]

Im Jahr 2022 hat Gartner die TEE-Technologie im Kontext von «Privacy-Enhancing-Computation» als technologischer Trend identifiziert. Unter «Privacy-Enhancing-Computation» sind Technologien zu verstehen, welche persönliche und sensible Informationen auf unterschiedlichen Infrastrukturen (Hardware, Software und Datenebene) schützen und einen sicheren Datenaustausch sowie Datenanalysen gewährleisten sollen.[83]

[78] KOHLBRENNER et al., S. 47 f.
[79] NIST, NIST IR 8320 Hardware-Enabled Security, S. 12.
[80] CCC, About the Confidential Computing Consortium.
[81] CCC, A Technical Analysis of Confidential Computing, S. 6.
[82] CCC, A Technical Analysis of Confidential Computing, S. 6.
[83] Gartner, Top Strategic Technology Trends for 2022.

Wird nun von ausserhalb des TEE versucht (bspw. von einem Betriebssystem aus), auf die TEE-Infrastruktur (Codes und Daten) zuzugreifen, wird dies blockiert.[84] Wie sich die Angriffsfläche mittels Einsatzes eines TEE verkleinert, ist in der Abb. 11 grafisch dargestellt.

Abb. 11: Angriffsfläche mit und ohne Confidential Computing mittels TEE



Anmerkung: POHLMANN, Confidential Computing, Intel SGX.

4.4 Forschungsstand

TEE geniessen in alltäglichen Produkten bereits eine grosse Anwendung. In modernen Smartphones sind Chips, welche auf der TEE-Technologie basieren, bereits im Gerät eingebaut. Das hat bspw. den Vorteil, dass biometrische Daten sowie Passwörter, welche in einem Smartphone gespeichert sind, geschützt werden.[85]

In den letzten Jahrzenten wurde viel Forschung im Bereich von TEE betrieben. Drei Versionen haben sich auf dem Markt durchgesetzt:

«Intel Software Guard Extensions»: Die von Intel entwickelte Version «Intel Software Guard Extensions» (Intel SGX) baut wie das TPM auf einer «Software Attestation» auf. Der Unterschied befindet sich jedoch in der Anzahl dieser durchgeführten Attestierungen. Während bei einem TPM alle laufenden Softwareanwendungen eines Computers mittels Attestierungen abgedeckt werden, befinden sich bei Intel SGX alle persönlichen Daten und die notwendigen Programmcodes innerhalb einer Enklave.[86]

In einer Intel SGX-Architektur gibt es einen nicht vertrauenswürdigen und einen vertrauenswürdigen Bereich. Der vertrauenswürde liegt innerhalb der Enklave und der nicht

[84] KOHLBRENNER et al., S. 48 f.
[85] Bern University of Applied Sciences, Course of Action.
[86] COSTAN/DEVADAS, S. 1 f.

vertrauenswürdige liegt im Betriebssystem. Nachdem Daten in einer Enklave bearbeitet wurden, werden diese entweder gelöscht oder durch eine Sealing-Funktion verschlüsselt auf der Festplatte gespeichert.[87]
Die innerhalb der Enklave gespeicherten Codes und Daten werden durch Intel SGX geschützt, indem bspw. Manipulationen, welche durch externe, nicht vertrauenswürdige Software ausgeführt werden möchte, verhindert oder abgebrochen werden.[88]
Sobald sich eine Enklave gegenüber einer sicheren Komponente als vertrauenswürdig bestätigt hat, wird ein verschlüsselter Kommunikations-Kanal erstellt, wobei sensible Daten in die Enklave geschleust werden können.[89]
Mit «Azure Confidential Computing» bietet Microsoft basierend auf dem Intel SGX-Chip seit 2017 eine Lösung an.[90]

ARM TrustZone: Die ARM TrustZone bietet eine Grundlage, auf welcher eine sichere und vertrauenswürdige Umgebung programmiert werden kann. Die Hardware in Form eines Chips, auch «Service on a Chip (SoC)» genannt, und die dazugehörige Software werden dabei in eine sichere und unsichere Umgebung unterteilt.[91]
Das Systemdesign stellt dabei sicher, dass ein Zugriff aus der unsicheren Umgebung in die sichere Umgebung unmöglich ist. Zu berücksichtigen ist diesem Kontext, dass die unsichere Umgebung keine Schwachstelle hat, sondern den Normalzustand beschreibt. Zwischen der nicht sicheren und der sicheren Welt besteht eine Beziehung, wobei ein Code in der sicheren Welt nur ausgeführt wird, wenn das Betriebssystem es mechanisch erlaubt.[92]

AMD Secure Encrypted Virtualization: Die AMD Secure Encrypted Virtualisation (SEV) von AMD ermöglicht die individuelle Verschlüsselung von Systemspeichern. So können virtuelle Maschinen voneinander isoliert werden. Die Schlüssel werden von der SEV verwaltet.[93] Im Jahr 2020 gab Google bekannt, dass sie die Lösung «Google Cloud Confidential Computing» basierend auf der SEV Technologie von AMD auf den Markt bringen.[94]

[87] HERFERT/LANGE/SPYCHALSKI, S. 131 f.
[88] MCKEEN, S. 1.
[89] Intel, Remote Attestation.
[90] RUSSINOVICH, Introducing Azure Confidential Computing.
[91] ARM, Building a Secure System, S. 3-2.
[92] ARM, Security in an ARMv8 System, S. 5.
[93] AMD, Secure Encrypted Virtualization (SEV).
[94] PORTER/LUGANI, Introducing Google Cloud Confidential Computing.

Google kommunizierte zudem, dass die Zukunft der Datenbearbeitung durch Verschlüsselung gegenüber dem Cloud-Anbieter oder Drittpersonen geprägt sein wird. Deswegen ist es zentral, die Daten vertrauenswürdig im Speicher zu verschlüsseln und den Schutz für die Privatsphäre der betroffenen Person sowie die Sicherheit der Daten während der Datenbearbeitung zu gewährleisten. Aktuell finden sehr viele Kollaborationen zwischen grossen Technologieunternehmen, wie bspw. Google und Intel, statt, welche zum Ziel haben, die Vertrauenswürdigkeit der Daten technisch auf noch höhere Niveaus anzuheben.[95] Nutzt man Confidential Computing, ist es nicht mehr notwendig, einem Cloud-Anbieter zu vertrauen. Man vertraut vielmehr dem TEE, welches in die CPU eingebaut ist und der eigenen Software, welche in der Enklave ausgeführt wird.[96]

4.5 Zwischenfazit Confidential Computing

Confidential Computing ermöglicht einen technischen Zugriffsschutz auf Daten in Bearbeitung. Die dafür notwendige vertrauenswürdige Umgebung wird durch Verschlüsselung und Attestation gewährleistet, wobei sichergestellt werden kann, dass kein Zugriff durch Administrierende oder Softwarebetreibende stattfinden kann und die Umgebung auf ihre Integrität geprüft wird.[97]

Das TEE macht die Datenbearbeitung in einer isolierten Umgebung, bzw. Enklave möglich. Die Codes und Daten, welche einen höheren Sicherheitsstandard benötigen, können durch das TEE vom restlichen Betriebssystem getrennt werden. Datenverschlüsselung, Datenintegrität und Code-Integrität sind Ansprüche, welche ein TEE sicherstellen muss. Die Angriffsfläche wird zudem erheblich verkleinert.[98]

Drei unterschiedliche Anbieter, darunter Intel mit dem Intel «SGX»-Chip, haben sich auf dem Markt durchgesetzt. Das Bedürfnis einer vertrauenswürdigen Verschlüsselung von Daten, welche den Zugriff durch Cloud-Anbieter und Drittpersonen verunmöglicht, wird zukünftig steigen.[99] Diese technischen Eigenschaften gilt es nun im Rahmen der gesetzlichen Anforderungen zu eruieren.

[95] POTTI/LUGANI, How Confidential Computing can transform cloud security.
[96] POHLMANN, Confidential Computing, Confidential Computing auf dem Punkt.
[97] Vgl. Kap. 4.2
[98] Vgl. Kap. 4.3
[99] Vgl. Kap. 4.4

II THEORETISCHER TEIL: Gesetzliche Grundlagen

Nachdem im ersten theoretischen Teil die technologischen Grundlagen erläutert wurden, folgt in einem weiteren Schritt die Betrachtung der rechtlichen Anforderungen, welche sich zur vorliegenden Thematik ergeben.

Gemäss Bundesverfassung hat jede Person den Anspruch auf Schutz der Privatsphäre.[100] Dieser Schutz ist weitergehend definiert durch die Achtung des Privat- und Familienlebens, des Wohnorts, der Kommunikation über den Brief-, Post und Fernmeldeverkehr[101] sowie den Schutz vor Missbrauch der persönlichen Daten.[102] Diese Grundrechte finden in Zeiten des Internets und der grossen digitalen Vernetzung wenig Raum, obwohl die Privatsphäre eine zentrale Rolle für die Erhaltung der Integrität jedes Einzelnen spielt. Nutzt man die Suchmaschine Google für eine Recherche zu einem Thema, ist diese Dienstleistung, welche Google erbringt, monetär unentgeltlich. Durch die Bestätigung der Allgemeinen Geschäftsbedingungen geben die Nutzenden ihr Einverständnis dafür, dass der Anbieter (in diesem Beispiel Google) datenschutzkonform die persönlichen Daten für Zwecke wie bspw. personalisierte Werbung oder den Verkauf an weitere Unternehmen nutzt. Im Zuge der Eigenverantwortlichkeit in der Handhabung der persönlichen Daten steht jedoch auch die Gesellschaft in der Verantwortung, die persönlichen Daten des Einzelnen zu schützen.[103] Der Datenschutz ist in der Schweiz im Bundesgesetz über den Datenschutz geregelt. Es hat zum Ziel, die personenbezogenen, bearbeiteten Daten der betroffenen Person so zu schützen, damit keine Grundrechte oder die Persönlichkeit verletzt werden.[104] Es stellt die gesetzliche Verankerung dieses Schutzes sicher. Das Bundesgesetz regelt die Bearbeitung von Personendaten von natürlichen Personen durch Private sowie durch Bundesorgane.[105]

In Kap. 5 werden die datenschutzrechtlichen Anforderungen für die Bearbeitung von Daten sowie die Gewährleistung der Datensicherheit detailliert erläutert. Die Begriffe «Verantwortlicher» und «Auftragsbearbeiter» werden für die Forschungsarbeit aus dem nDSG übernommen.

[100] Art. 13 Abs. 1 BV.
[101] Art. 13 Abs. 2 BV.
[102] Art. 13 Abs. 3 BV.
[103] POHLMANN, S. 20.
[104] Art. 1 nDSG.
[105] Art. 2. Abs. 1 nDSG.

5 Das neue Bundesgesetz über den Datenschutz (nDSG)

Personenbezogene Daten spielen in der Wirtschaft eine zentrale Rolle. Unternehmen haben einen grossen Anreiz, möglichst viele Personendaten zu sammeln, um so das Konsumverhalten zu erfassen und die unternehmerische Strategie gezielt darauf auszurichten. Das kann so weit gehen, dass der Alltag einer Person nachgezeichnet und damit Vorlieben, Freizeitaktivitäten oder auch Infos zu Versicherungsleistungen und Ferienplanung in Erfahrung gebracht werden können. Aufgrund der gegebenen Attribute lassen sich die Personen anschliessend in Gruppen kategorisieren. Dieser gesamte Prozess verläuft im Hintergrund und die meisten Personen wissen darüber nicht Bescheid. In einer Demokratie und einer rechtsstaatlichen Gesellschaft bildet jedoch das informationelle Selbstbestimmungsrecht einen wichtigen Grundsatz. Dabei tangiert dieser Grundsatz nicht nur den bereits erwähnten wirtschaftlichen Bereich, sondern auch die gesundheitlichen und staatlichen Institutionen. Das informationelle Selbstbestimmungsrecht[106] zu schützen und die Verhältnismässigkeit der gesammelten Daten zu wahren, ist das primäre Ziel des Datenschutzes.[107]

Mit der Totalrevision des Datenschutzgesetzes nähert sich die Schweizer Gesetzgebung der EU-Datenschutzgrundverordnung (DSGVO) an. Diese Revision war aufgrund der technologischen Entwicklungen und den gesellschaftlichen Veränderungen notwendig. Ausschlagegebend für die Anpassungen des Schweizer Datenschutzgesetzes war zudem auch das revidierte Übereinkommen SEV 108. Mit der Totalrevision wird die Schweiz von der EU fortan als Land, welches einen angemessenen Datenschutz gewährleistet, angesehen, was die Zusammenarbeit erleichtert. [108] Das neue Datenschutzgesetz (nDSG) tritt am 1. September 2023 in Kraft.[109] Die darin enthaltenen gesetzlichen Verankerungen werden in der Datenschutzverordnung (DSV) konkretisiert.

5.1 Geltungsbereich

Das nDSG regelt die Bearbeitung von personenbezogenen Daten, wenn diese Bearbeitung durch Private[110] oder Bundesorgane[111] durchgeführt wird. Territorial hat das nDSG Gültigkeit für Sachverhalte, welche einen Einfluss in der Schweiz ausüben. Das bedeutet, ein in der Schweiz relevanter Sachverhalt könnte auch im Ausland ausgelöst werden.[112]

[106] Vgl. Art. 13 Abs. 2 BV.
[107] EDÖB, Datenschutz.
[108] EDÖB, Stärkung des Datenschutzes, Worum geht es?
[109] WBF, Neues Datenschutzgesetz (revDSG).
[110] Art. 2. Abs. 1 lit. a. nDSG.
[111] Art. 2. Abs. 1 lit. b. nDSG
[112] Art. 3. Abs 1 nDSG.

Schweizer Unternehmen können unter gewissen Umständen jedoch von den Richtlinien der DSGVO betroffen sein.[113] Dieser Fall trifft ein, wenn personenbezogene Daten von Personen, welche sich in der Europäischen Union (EU) befinden, verarbeitet werden und bezweckt wird, Waren oder Dienstleistungen an natürliche Personen in der EU anzubieten oder deren Verhalten zu ermitteln.[114]

5.2 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)

In der Schweiz existiert mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eine Behörde, welche im Bereich des Datenschutzes, Datenbearbeitungen durch die Bundesverwaltung und durch Private beaufsichtigt und beratend zur Verfügung steht.[115] Bei Datenschutzverletzungen, welche eine grosse Anzahl an personenbezogenen Daten betreffen könnten, kann der EDÖB innerhalb seiner Beaufsichtigungspflicht einschreiten.[116]

5.3 Relevante Datenschutzbestimmungen

Damit die zugrundeliegende Thematik einer rechtlichen Analyse unterzogen werden kann, werden in den folgenden Abschnitten die rechtlichen Bestimmungen der Datenbearbeitung durchleuchtet und deren Relevanz für die vorliegende Thematik aufgezeigt.

5.3.1 Personendaten

Im nDSG werden Personendaten als «alle Angaben, welche sich auf eine bestimmte oder bestimmbare natürliche Person beziehen» definiert.[117] Die Klassifizierung der besonders schützenswerten Personendaten ist zudem auch zu berücksichtigen. Darunter verstehen sich[118]:

- Daten zu religiösen, politischen und gewerkschaftlichen Einstellungen und Tätigkeiten.
- Daten aus dem Gesundheitsbereich, intime oder ethnische Daten sowie genetische Daten.
- Daten, welche Aussagen über die Biometrie einer Person zulassen und eine eindeutige Identifikation ermöglichen.

[113] EDÖB, Tipps zur DSGVO.
[114] Art. 3 DSGVO
[115] EDÖB, Auftrag & Aufgaben.
[116] EDÖB, Aufgaben des EDÖB.
[117] Art. 5 lit. a nDSG
[118] Art. 5 lit. c Z.1-6 nDSG

- Daten aus Gründen von verwaltungs- oder strafrechtlichen Ereignissen.
- Daten über die Beanspruchung der Sozialhilfe.

Die Bestimmungen sind jedoch nicht eindeutig abgrenzbar, wie sich am Beispiel der Gesundheitsdaten zeigt. Bei Gesundheitsdaten handelt es sich um besonders schützenswerte Personendaten, sofern sie einer bestimmbaren und natürlichen Person zugeordnet werden können. Da jedoch im nDSG keine Legaldefinition von Gesundheitsdaten vorhanden ist, ergibt sich aus dem gesetzlichen Rahmen kein absolutes Verständnis. Deswegen wird der Kontext der Datenbearbeitung in den Vordergrund gerückt. Dabei ergibt sich jedoch bereits die nächste Unsicherheit in der Definition der Begrifflichkeiten der Gesundheitsdaten sowie den genetischen und biometrischen Daten. Dieser erschwerte Umgang mit Gesundheitsdaten ist in der Praxis spürbar und ist für die Innovationskultur im Gesundheitssektor nicht förderlich. Für eine klar abgrenzbare Betrachtung von Gesundheitsdaten reicht das nDSG somit nicht aus.[119]
Ähnlich ist die Situation bei der Bestimmbarkeit einer Person, welche im Art. 5 lit. a nDSG ausgeführt wird. Gemäss der DSGVO bedingt die Feststellung, ob eine natürliche Person identifizierbar ist, die Berücksichtigung «aller Mittel», welche durch einen Verantwortlichen oder andere Personen genutzt werden könnten, um eine natürliche Person auf direktem oder indirektem Wege, wie bspw. durch das «Aussondern» zu identifizieren.[120] Das nDSG bietet grossen Spielraum bei der Betrachtung, dass die durch eine Pseudonymisierung erstellen Kenndaten mittels «Aussondern» keine Personendaten darstellen, sofern die durch die Pseudonymisierung erstellten Daten keine natürliche Person identifizierbar machen oder diese Person identifiziert ist.[121] Im Kap. 5.7 wird diese Thematik noch genauer erläutert. Vorab muss jedoch der Begriff der Datenbearbeitung sowie die Datenbearbeitungsprinzipien geklärt werden.

5.3.2 Datenbearbeitung

Es gilt zu unterscheiden, dass in der Schweizer Gesetzgebung von «Bearbeitung[122]» und in der DSGVO von einer «Verarbeitung[123]» gesprochen wird. Die vorliegende Forschung ist mit Fokus auf die Schweizer Gesetzgebung verfasst, weshalb fortan der Begriff «Datenbearbeitung» verwendet wird.

[119] WIDMER/BÜHLMANN et. al, S. 15-18.
[120] DSGVO, Erwägungsgrund 26 Abs. 3.
[121] WIDMER/BÜHLMANN et. al, S. 9 f.
[122] Art. 5 lit. d nDSG
[123] Art. 4 Abs. 2 DSGVO

An einer Datenbearbeitung ist zum einen die betroffene Person («Data subject») und zum anderen der Verantwortliche («Controller») involviert. Gegebenenfalls wird ein Auftragsbearbeiter («Processor») beigezogen. Innerhalb der Datenbearbeitung sollen die beiden letzteren Parteien so handeln, dass der Datenschutz pflichtgemäss eingehalten wird.[124] Diese Thematik wurde bereits in Kap. 3.1 im Kontext der Cloud erläutert.
Unter einer Bearbeitung versteht sich «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten».[125] Die Datenbearbeitung bezieht sich auf sämtliche (automatisierte) Prozesse oder Prozessreihen, welche mit personenbezogenen Daten in Zusammenhang stehen.[126]
In der Datenbearbeitung gelten gemäss Art. 6 Abs. 1 bis 5 nDSG folgende Grundsätze:

- Rechtmässigkeit
- nach Treu und Glauben und verhältnismässig
- Zweckmässigkeit (sobald der Zweck nicht mehr vorhanden, werden die Daten vernichtet oder anonymisiert)
- Richtigkeit

Sofern Einwilligung für die Datenbearbeitung notwendig ist, muss diese freiwillig erteilt werden.[127] Die Persönlichkeit einer betroffenen Person kann verletzt werden, wenn besonders schützenswerte Personendaten an Dritte bekanntgegeben werden, ohne eine Einwilligung der betroffenen Person eingeholt zu haben. [128] Die Regel besagt, dass keine Persönlichkeitsverletzung vorliegt, sofern die betroffene Person einer Bearbeitung zugesagt und Zugang zu den Personendaten gewährt hat.[129]
Wird ein Profiling von besonders schützenswerten, personenbezogenen Daten durch Private oder Bundesorgane durchgeführt, muss eine Einwilligung für die Bearbeitung erfolgen.[130] Unter einem Profiling versteht sich eine automatisierte Bearbeitung von personenbezogenen Daten. Das beinhaltet u.a. die Verwendung von personenbezogenen Daten, um ein persönliches Verhalten unterschiedlicher Lebensbereiche von natürlichen Personen zu bewerten, Interessen zu ermitteln, psychische und demografische Eigenschaften sowie ökonomische Gegebenheiten zu analysieren und vorherzusagen.[131]

[124] SCHÖNBÄCHLER, S. 174 f.
[125] Art. 5 lit. d nDSG
[126] EDPS, Datenverarbeitung dokumentieren, S. 7.
[127] Art. 6 Abs. 6 nDSG
[128] Art. 30 Abs. 2 lit c. nDSG
[129] Art. 30 Abs. 3 nDSG
[130] Art. 6 Abs. 7 nDSG
[131] Art. 4 Abs. 4 DSGVO

Im nDSG ist neu geregelt, dass Verantwortliche und Auftragsbearbeiter über alle Bearbeitungstätigkeiten ein Verzeichnis führen müssen.[132] Im Verzeichnis muss dokumentiert sein, wer der Inhaber ist, was der Zweck der Bearbeitung beinhaltet, welche Personen mit welchen Daten betroffen sind, an wen die Daten weitergeleitet werden und wie lange diese Daten aufbewahrt werden.[133] Zudem müssen die geeigneten Massnahmen zur Einhaltung der Datensicherheit[134] und bei Bekanntgabe ins Ausland die Angaben zum Staat sowie vereinbarte Garantien ersichtlich sein.[135] Für Auftragsbearbeiter gelten gemäss Art. 12 Abs. 3 nDSG die gleichen Anforderung mit minimalen Anpassungen. Von dieser Richtlinie ausgenommen sind Unternehmen, welche weniger als 250 Mitarbeitende führen und keine Datenbearbeitungen durchführen, welche mit hohen Risiken für Datenschutzverletzungen in Verbindung sind.[136]

5.3.3 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Die Grundsätze der Bearbeitung von personenbezogenen Daten müssen durch technische und organisatorische Massnahmen (TOM), welche bereits ab dem Zeitpunkt der Planung einer Datenbearbeitung ausgestaltet werden, eingehalten werden.[137]

Der Datenschutz durch Technik («Privacy by Design»[138]), schützt mittels Einbezugs der Art und des Umfangs der Datenbearbeitung die personenbezogenen Daten angemessen vor Risiken.[139] Das bedeutet, dass nebst technischen Gegebenheiten von Computer auch alle Prozesse, welche die Datenbearbeitung tangieren, berücksichtigt werden müssen.[140] Eine technische Verschlüsselung sorgt bspw. dafür, dass Nachrichten von unbefugten Personen nicht gelesen werden können. Datenschutz durch Technik schützt die Privatsphäre von betroffenen Personen und garantiert die Einhaltung der Grundsätze des Datenschutzes.[141]

Datenschutzfreundliche Voreinstellungen («Privacy by Default»[142]) stellen sicher, dass keine unbefugten Personen Zugang zu personenbezogenen Daten erhalten, zu welcher die betroffene Person nicht zugestimmt hat. Der Gesetzgeber reduziert die Menge der

[132] Art. 12 Abs. 1 nDSG
[133] Art. 12 Abs. 2 lit. a-e nDSG
[134] Art. 12 Abs. 2 lit f. nDSG
[135] Art. 12 Abs. 2 lit g. nDSG
[136] Art. 12 Abs. 5 nDSG
[137] Art. 7 Abs. 1 nDSG
[138] STECKLER/KREMPEL, S. 79 f.
[139] Art. 7 Abs. 2 nDSG
[140] ROSENTHAL, RN 45.
[141] Europäische Kommission, Was bedeutet „Datenschutz durch Technikgestaltung“ und „durch datenschutzfreundliche Voreinstellungen“?.
[142] STECKLER/KREMPEL, S. 79 f.

bearbeiteten Personendaten auf ein Minimum, sodass der bestimmte Zweck jedoch noch eingehalten werden kann.[143] «Privacy by Default» soll die betroffenen Personen auch vor einem allfälligen Fehlgebrauch einer Anwendung schützen.[144]
Bei der Nutzung von sozialen Medien sollen bspw. die Standardeinstellungen auf ein Mindestmass reduziert sein, was den Zugang zu einem Profil einschränkt und eine Verbreitung der personenbezogenen Daten an eine unbestimmte Anzahl Personen verhindert.[145]

5.3.4 Datensicherheit und Meldepflicht

Verantwortliche und Auftragsbearbeiter werden in Bezug auf die Gewährleistung von Datensicherheit mittels dafür brauchbaren technischen und organisatorischen Massahmen per Gesetz direkt verpflichtet.[146] «Diese Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden».[147] Zudem hat der Bundesrat Minimalanforderungen an die Datensicherheit festgelegt.[148] Damit jene Massnahmen durch Verantwortliche sowie Auftragsdatenbearbeiter entsprechend getroffen werden können, müssen vorher der Schutzbedarf der Daten und vorhandene Risiken evaluiert werden.[149]
Wird eine Schutzbedarfsanalyse durchgeführt, müssen die folgenden Kriterien berücksichtigt werden:

- Art der bearbeiteten Daten: Der Verantwortliche und der Auftragsbearbeiter müssen prüfen, ob es sich bei den betroffenen Personendaten um besonders schützenswerte Daten gemäss Art. 5 lit. c nDSG handelt.[150]
- Zweck, Art, Umfang und die Umstände der Bearbeitung: Der Zweck beinhaltet nicht nur den Zweck der Datenbearbeitung, sondern auch die Überprüfung, ob zur Einhaltung der Grundrechte sowie der Persönlichkeitsrechte ein erhöhtes Risiko besteht.[151]

  Die Art der Bearbeitung beschreibt, wie die Daten bearbeitet werden. Wird die Datenbearbeitung durch automatisierte Prozesse (mittels künstlicher Intelligenz) ausgeführt, kann der Schutzbedarf höher eingestuft werden. Der Umfang

[143] Art. 7 Abs. 3 nDSG
[144] STECKLER/KREMPEL, S. 79 f.
[145] Europäische Kommission, Was bedeutet „Datenschutz durch Technikgestaltung“ und „durch datenschutzfreundliche Voreinstellungen“?.
[146] Art. 8 Abs. 1 nDSG
[147] Art. 8 Abs. 2 nDSG
[148] Art. 8 Abs. 3 nDSG
[149] Art. 1 Abs. 1 DSV
[150] Art. 1 Abs. 2 lit. a DSV
[151] Art. 1 Abs. 2 lit. b DSV

beschreibt die Anzahl der Personen, welche durch eine Datenbearbeitung betroffen sind. Veranschaulichen lässt sich das bspw. mit der Überwachung von öffentlichen Bereichen, welche eine umfangreiche Datenbearbeitung auslöst. Die Umstände der Datenbearbeitung beschreiben Aspekte, welche die restlichen Kriterien beeinflussen können. Der Gesetzgeber ermöglicht somit die Ergänzung von weiteren Kriterien, welche keinem bestehenden Kriterium untergeordnet werden können. Wird eine Datenbearbeitung bspw. in einer Cloud durchgeführt, untersteht sie einem höheren Schutzbedarf, als wenn sie auf einem internen Server erfolgt, auf welchen externe keinen Zugriff haben.[152]

Die DSV präzisiert zudem, dass die Daten nur an Personen zugänglich gemacht werden dürfen, welche eine Berechtigung haben[153] und nur verfügbar sind, wenn Notwendigkeit besteht.[154] Zudem wird der Schutz vor beabsichtigter oder unbeabsichtigter Veränderung gewahrt[155] und die Daten müssen nachvollziehbar bearbeitet werden.[156] Die technischen und organisatorischen Massnahmen müssen in einem solchen Masse erhoben werden, damit eine Datensicherheitsverletzung vermieden wird.[157] Konkrete Massnahmen, resp. Mindestanforderungen zum Schutz der Datensicherheit werden jedoch durch den Gesetzgeber nicht formuliert. Die Anforderungen lassen sich unter dem Grundsatz von «Privacy by Design» einordnen.[158]

Im Fokus steht die Berücksichtigung des Verhältnisses zwischen dem Schutz und dem Risiko, welche die personenbezogenen Daten ausgesetzt sind. Das bedeutet, dass das Gesetz keinen absoluten Schutz verlangt.[159]

Der Verantwortliche muss eine Verletzung der Datensicherheit so schnell wie möglich dem EDÖB melden, sofern ein hohes Risiko für die Grundrechte oder für die Persönlichkeit der betroffenen Person entstehen könnte.[160] Dasselbe gilt für den Auftragsbearbeiter, welcher die Verletzung an den Verantwortlichen rapportieren.[161]

[152] EJPD, S. 19.
[153] Art. 2 lit. a DSV
[154] Art. 2 lit. b DSV
[155] Art. 2 lit. c DSV
[156] Art. 2d DSV
[157] Art. 8 Abs. 2 nDSG
[158] MEYLE/MORAND/VASELLA.
[159] ROSENTHAL, RN 55.
[160] Art. 24 Abs. 1 nDSG
[161] Art. 24 Abs. 3 nDSG

5.3.5 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) ist ein Prozess, der Verantwortliche im Umgang mit Risiken, welche durch eine Datenbearbeitungsprozess verursacht werden, unterstützt.[162] Ist eine Datenbearbeitung mit höheren Risiken für den Datenschutz verbunden, wird die DSFA als Instrument zur «datenschutzrechtlichen Selbstbeurteilung» genutzt.[163]

Die DSFA ist in Artikel 22 nDSG verankert. Der Verantwortliche erstellt vor einer geplanten Datenbearbeitung eine DSFA, wenn aus der Datenbearbeitung erhöhte Risiken für die Grundrechte oder die Persönlichkeit der betroffenen Person resultieren.[164] Dabei ergeben sich hohe Risiken insbesondere bei der Verwendung von neuen Technologien, was alte Technologien jedoch nicht ausschliesst.[165] Ein hohes Risiko entsteht, wenn eine grosse Menge an besonders schützenswerten Daten bearbeitet wird[166] oder wenn öffentliche Bereich systematisch und umfangreich überwacht werden.[167]

Eine DSFA spiegelt wider, um welche Bearbeitung es sich handelt und wie die Risiken bewertet werden. Auf Basis der Risikobewertung werden Massnahmen definiert, welche die ermittelten Risiken minimieren können.[168] Die Risiken können entweder durch bestehende oder zukünftig eingesetzte TOM aufgehoben oder wenigstens angemessen reduziert werden.[169]

Wird bei der Erfassung der Risiken, welche sich durch eine Datenbearbeitung für betroffene Personen ergeben, strukturiert vorgegangen, unterstützt die Erstellung einer DSFA Unternehmen bei der Einhaltung von «Privacy by Design» und somit bei der Umsetzung der technischen Massnahmen.[170]

Birgt die geplante Datenbearbeitung trotz den, aufgrund der durchgeführten DSFA, geplanten Massnahmen ein hohes Risiko für die Grundrechte oder die Persönlichkeit der betroffenen Person, ist der Verantwortliche dazu verpflichtet, dies vor der Umsetzung der geplanten Datenbearbeitung dem EDÖB zu melden und eine entsprechende Stellungnahme einzufordern.[171] Der EDÖB wird die Meldung innerhalb von zwei Monaten

[162] EDPS, Datenschutz-Folgenabschätzung (DSFA).
[163] ROSENTHAL, N 148.
[164] Art. 22 Abs. 1 nDSG
[165] Art. 22 Abs. 2 nDSG
[166] Art. 22 Abs. 2 lit a. nDSG
[167] Art. 22 Abs. 2 lit b. nDSG
[168] Art. 22 Abs. 3 nDSG
[169] ROSENTHAL, N 150.
[170] EDPS, Datenschutz-Folgenabschätzung.
[171] Art. 23 Abs 1 nDSG

bearbeiten und seine Bedenken mitteilen[172] und unter Umständen geeignete Massnahmen vorschlagen.[173]

5.3.6 Auftragsbearbeitung

Wie es der Begriff bereits beschreibt, handelt es sich bei der Auftragsbearbeitung um eine Datenbearbeitung, welche durch den Verantwortlichen an einen Dritten, d.h. einem Privaten (bspw. ein Unternehmen) oder an eine Bundesbehörde, ausgelagert wird.[174] Hat ein Unternehmen bspw. keine internen IT-Unterhalts-Kompetenzen, können diese Aufgaben an einen Anbieter ausgelagert werden.[175]

Das Gesetz schreibt vor, dass bei einer Bearbeitung durch Dritte die Daten so bearbeitet werden, wie der Verantwortliche die Datenbearbeitung durchführen dürfte.[176] Zudem darf keine vertragliche oder gesetzliche Geheimhaltungspflicht ein Verbot der Übertragung verursachen.[177] Der Verantwortliche muss sicherstellen, dass der Auftragsbearbeiter die Datensicherheit entsprechend gewährleisten kann.[178] Zu diesem Zweck müssen vorab mittels einer Risikoanalyse rechtliche Aspekte geklärt sowie technische und organisatorische Gegebenheiten eruiert werden.[179] Das bedeutet, dass der Verantwortliche die Wahl des Auftragsbearbeiters mit Sorgfalt fällt und mittels Vertrags sicherstellen muss, dass der Auftragsbearbeiter über die zu bearbeitenden Daten entsprechend instruiert wurde und die Umsetzung der Dienstleistung überwacht wird, damit der Verantwortliche in seinem Handeln datenschutzkonform bleibt.[180] Wenn der Auftragsbearbeiter die Bearbeitung auf Dritte übertragen möchte, muss der Verantwortliche dies vorher genehmigen.[181] Aufgrund der Konstellation des Datenverantwortlichen, welcher die eigenen Daten zur Bearbeitung an den Auftragsbearbeiter auslagert, handelt es sich um einen Auftrag «nach Weisung». Die Auslagerung von Leistungen an einen Cloud-Dienst ist ein typisches Beispiel für die Auftragsbearbeitung. Der Verantwortliche wählt bei der Auslagerung die entsprechende Software und Services selbst aus. Rosenthal vergleicht das Verhältnis zwischen dem Verantwortlichen der Daten und dem Anbieter mit einem Gast im Restaurant, welcher aus der Speisekarte etwas bestellen kann, wenn er möchte.[182]

---

[172] Art. 23 Abs 2 nDSG
[173] Art. 23. Abs. 3 nDSG
[174] Art. 5 lit. k nDSG
[175] ROSENTHAL, N 57.
[176] Art. 9 Abs. 1 lit. a nDSG
[177] Art. 9 Abs. 1 lit. b nDSG
[178] Art. 9 Abs. 2 nDSG
[179] HOFFMANN, S. 466.
[180] ROSENTHAL, N 59.
[181] Art. 9 Abs. 3 nDSG
[182] ROSENTHAL, N 15.

5.3.7 Datenbearbeitung durch private Personen – Besondere Bestimmungen

Sofern personenbezogene Daten durch Private bearbeitet werden, gelten besondere Bestimmungen. So darf eine Datenbearbeitung «die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen».[183]

«Widerrechtlich» bedeutet:

- gegen die in Art. 6 und Art. 8 nDSG existierenden Grundsätze der Datenbearbeitung, gegen den Willen der betroffenen Person sowie wenn besonders schützenswerte Daten an Dritte bekanntgegeben werden.[184]
- sofern die Datenbearbeitung «nicht durch Einwilligung der betroffenen Person», oder durch übergeordnetes Interesse oder gesetzliche Grundlage gerechtfertigt werden kann.[185]

5.4 Zertifizierung

Datenbearbeitungssysteme, -produkte und -dienstleistungen können durch unabhängige Prüfgesellschaften zertifiziert werden.[186] Der Hersteller, der Verantwortliche sowie der Auftragsbearbeiter müssen jedoch den Anforderungen an die Zertifizierungsverfahren, welche durch den Bundesrat festgelegt wurden, Folge leisten, damit die Zertifizierungen auch anerkannt werden.[187] Dienstleistungen wurden mit der Revision des Datenschutzgesetzes neu aufgenommen. Dieser Zusatz soll für mehr Nachvollziehbarkeit in der Datenbearbeitung sorgen sowie das Risiko verringern, dass sich Datenschutzvorfälle ereignen. Nicht zuletzt sorgt dieser Aspekt bei den Konsumenten für mehr Vertrauen in eine Dienstleistung. Sofern eine entsprechende Zertifizierung für eine Datenbearbeitung besteht, entfällt die Durchführung der Datenschutz-Folgenabschätzung (vgl. Kap. 5.3.5), da ein Zertifizierungsverfahren dieselbe Prüfung einer Datenbearbeitung beinhaltet.[188] Eine detaillierte Ausführung der Verordnung über die Datenschutzzertifizierungen wird aus Gründen des Forschungsrahmens verzichtet.

5.5 Geheimhaltung und Schweigepflicht

Wird ein Beruf ausgeübt, welcher der beruflichen Schweigepflicht unterliegt, muss man nebst datenschutzrechtlichen Prüfungen auch strafrechtliche Prüfungen sowie

[183] Art. 30 Abs. 1 nDSG
[184] Art. 30 Abs. 2 lit. a-c nDSG
[185] Art. 31 Abs. 1 nDSG
[186] Art. 13 Abs. 1 nDSG
[187] Art. 13 Abs. 2. nDSG
[188] ECKERT/IMFELD, S. 12.

branchenrelevante weitere Prüfungen durchführen, um herauszufinden, ob die Nutzung von Technologien wie der Cloud erlaubt ist.[189] Die Berufliche Schweigepflicht ist im Strafgesetzbuch geregelt.[190] Aus datenschutzrechtlicher Sicht werden bei einem Verstoss gegen die berufliche Schweigepflicht auf Antrag Bussen bis zu 250'000 Franken erhoben.[191]

5.6 Bussgelder

In Kap. 5.3.6 wurde ersichtlich, dass der Verantwortliche mittels Vertrags mit dem Auftragsbearbeiter die Umsetzung der Datenbearbeitung sorgfältig sicherstellen muss. Kommt der Verantwortliche seiner Pflichten nicht nach, kann für einen Verstoss bis zu 250'000 Franken Busse gesprochen werden. Die Bussen werden bei Verstössen gegen die Grundsätze der Bekanntgabe von Personendaten ins Ausland[192], bei Widerhandlungen hinsichtlich der Bearbeitung durch Auftragsbearbeiter sowie bei ungenügender Datensicherheit angewendet.[193]

5.7 Anonymisierte und pseudonymisierte Datenbearbeitung

Anonymisierte Daten sind Daten, welcher keiner natürlichen Person zugeordnet werden können oder die Zuordnung nur mittels eines unverhältnismässig hohen Aufwands möglich ist. Bei einer Pseudonymisierung werden die personenbezogenen Daten durch eine sogenannte «Korrespondenztabelle» neutralisiert. Die ursprünglichen Daten sind durch die entsprechende «Korrespondenztabelle» wiederherstellbar.[194]

Sofern eine Datenbearbeitung nicht zu einem personenbezogenen Zweck verfolgt wird, was unter anderen in der Forschung der Fall ist, sieht der Gesetzgeber vor, dass Datenbearbeitungen auch ohne Einwilligung gerechtfertigt sein können. Im nDSG wird vorausgesetzt, dass die Daten anonymisiert werden oder, sofern der Aufwand dafür unangemessen hoch ist, die Bestimmbarkeit der betroffenen Personen verhindert wird.[195] Zudem dürfen «besonders schützenswerte Personendaten» nur an Dritte weitergegeben werden, sofern diese eine betroffene Person nicht bestimmbar machen oder zumindest die Bearbeitung keinen personenbezogenen Zweck verfolgt.[196] Als dritte Voraussetzung gilt es,

[189] HÜRLIMANN/STEIGER, S. 199.
[190] Art 321 StGB
[191] Art. 62 Abs. 1 nDSG
[192] Art. 61 lit. a nDSG
[193] Art. 61 nDSG
[194] EDÖB, Datenschutz und Forschung im Allgemeinen.
[195] Art. 31 Abs. 2 lit. e Ziff. 1 nDSG
[196] Art. 31 Abs. 2 lit. e Z. 2 nDSG

die Veröffentlichung der Ergebnisse so zu gestalten, dass die betroffenen Personen nicht identifiziert werden können.[197] In Bezug auf die Sekundärnutzung von Personendaten ist der letzte Rechtfertigungsgrund zentral.[198] Zu beachten gilt in diesem Kontext jedoch, dass im Forschungsbereich, insbesondere in der Humanforschung das Humanforschungsgesetz (HFG) gegenüber dem nDSG Vorrang hat.[199]

In der Praxis gibt es heutzutage viel mehr Akteure, welche Gesundheit- oder «Lifestyle-Daten» bearbeiten. War es früher noch der behandelnde Arzt, welcher Gesundheitsdaten erfasste, finden wir bspw. mit Google und Apple grosse Mitspieler im Bereich der Bearbeitung der Gesundheitsdaten. Dabei kommt es jedoch immer auf den Kontext an, ob Daten als Gesundheitsdaten klassifiziert werden oder nicht. Die Daten, welche mittels einer Sportuhr gesammelt werden, können für einen Patienten als Gesundheitsdaten, aber für einen gesunden Menschen als «Lifestyle-Daten» klassifiziert werden.[200]

Es stellt sich jedoch die Frage, inwiefern heutzutage personenbezogene Daten insbesondere Gesundheitsdaten noch anonymisiert bzw. anonym sind. In der Forschung werden sehr viele genetischen Daten gesammelt, welche aufgrund der Individualität eine einfachere Re-Identifikation erlauben.[201] Die Art der Datennutzung ist auch im Parlament ein Thema. Dazu folgt im nächsten Abschnitt ein kurzer Aktualitätsbezug

5.8 Nutzung von Sekundärdaten - Ein Aktualitätsbezug

Die Kommission für Wissenschaft, Bildung und Kultur hat im August 2022 eine Motion eingereicht, welche eine gesetzliche Regelung der Nutzung von Sekundärdaten fordert. In der Motion wird für eine effizientere Nutzung von Daten appelliert. Durch die Konsolidierung unterschiedlicher Daten in sogenannten «Datenräumen» kann ein neuer, sekundärer Nutzen generiert werden. Dies kann bspw. in der Forschung zu neuen Erkenntnissen führen. Damit man die Daten sekundär nutzen kann, bedarf es jedoch zuerst der Schaffung von vertrauenswürdigen «Datenräumen». Aus technologischer Sicht gibt es einige Optionen, welche dies anbieten. Zurzeit fehlt es eher an gesetzlichen Rahmenbedingungen, nach denen man sich richten könnte.[202]

Die Sekundärnutzung von Gesundheitsdaten ist jedoch durch ein komplexes Umfeld geprägt. Bei Gesundheitsdaten handelt es sich einerseits um besonders schützenswerte

[197] Art. 31 Abs. 2 lit. e Z. 3 nDSG
[198] ROSENTHAL, N 42.
[199] ROSENTHAL, N 42.
[200] VOKINGER, N 22 f.
[201] VOKINGER, N 20.
[202] Kommission für Wissenschaft, Bildung und Kultur, Mo. Ständerat (WBK-SR), S. 2.

Daten aus einem Bereich, welcher stark reguliert ist. Obwohl anonymisierte Daten keinen Personenbezug mehr aufweisen, ist eine Re-Identifizierung bei Gesundheitsdaten im Verhältnis einfacher durchzuführen. Personenbezogene Daten, welche genetische Informationen beinhalten, lassen sich nur schwer oder gar nicht anonymisieren.[203]
Die Herausforderung der Anonymisierung von Sekundärdaten im Gesundheitsbereich wurde durch ein Gutachten beurteilt. Dieses legte dar, dass Confidential Computing durchaus eine Möglichkeit darstellt, mittels technischer Verschlüsselung die Anonymisierung aufrechtzuerhalten.[204]

5.9 Bekanntgabe von Personendaten ins Ausland

Möchte ein Unternehmen interne Personendaten an Dritte im Ausland auslagern, ist dies zulässig, sofern der Bundesrat beschlossen hat, dass das betreffende Land einen angemessenen Datenschutz sicherstellt.[205]
Als Hilfsmittel für einen sicheren Datentransfer ins Ausland findet sich neu im Anhang 1 der DSV eine Aufstellung der Länder, welche gemäss Bundesrat einen angemessenen Datenschutz aufweisen.[206] Darin lässt sich entnehmen, dass die USA nicht zu den Staaten mit einem angemessenen Datenschutz gehören. In periodischen Abständen wird eine Neubeurteilung der Angemessenheit des Datenschutzes durchgeführt[207] und veröffentlich [208] Eine Neubeurteilung kann Änderungen der Aufstellung im Anhang 1 der DSV mit sich ziehen, welche jedoch keine bereits durchführten Datenbekanntgaben tangieren.[209]
Werden die Daten einem Land bekanntgegeben, welches gemäss den Entscheidungen des Bundesrats keinen angemessenen Datenschutz vorweisen kann, kann die Bekanntgabe ins Ausland basierend auf einem angemessenen Datenschutz trotzdem erfolgen, wobei der Datenschutz durch einen völkerrechtlichen Vertrag, durch Datenschutzklauseln oder spezifischen Garantien, Standarddatenschutzklauseln (engl. Standard Contractual Clause, SCC) oder Datenschutzvorschriften, welche intern verbindlich sind, gewährleistet werden muss. Zu beachten ist, dabei, dass der EDÖB vorgängig eine Genehmigung für die angewendeten Garantien, Standarddatenschutzklauseln sowie für bindenden internen Datenschutzvorschriften ausgesprochen haben muss.[210]

[203] SATW, Empfehlungen, S. 21.
[204] WIDMER/BÜHLMANN et. al., S. 11.
[205] Art. 16 Abs. 1 nDSG
[206] Art. 16 Abs. 1 nDSG; Art. 8 Abs. 1 DSV
[207] Art. 8 Abs. 4 DSV
[208] Art. 8 Abs. 5 DSV
[209] Art. 8 Abs. 6 DSV
[210] Art. 16 Abs. 2 lit. a-e nDSG

Die Standarddatenschutzklauseln werden im folgenden Abschnitt detaillierter erläutert.

5.9.1 Standarddatenschutzklauseln

Plant ein Schweizer Unternehmen, Personendaten in ein Land ohne angemessenen Datenschutz zu übermitteln, müssen SCC vereinbart werden, welche sich auf Schweizer Recht abstützen.[211] Der EDÖB stellt eine Liste mit SCC öffentlich zur Verfügung. Diese wurden durch den EDÖB genehmigt, ausgestellt oder anerkannt. Weitere eingereichte Standarddatenvertragsklauseln werden durch ihn geprüft und das Ergebnis innerhalb von 90 Tagen mitgeteilt.[212]

Der EDÖB genehmigt Standardvertragsklauseln, welche unter Berücksichtigung der DSGVO von der Europäischen Kommission bereits anerkannt wurden. Zudem müssen bei einer Speicherung von Personendaten auf der Cloud, unabhängig davon, ob das Land einen angemessenen Datenschutz bietet oder nicht, die betroffenen Personen über die Bekanntgabe ins Ausland informiert werden.[213] Microsoft bietet für die Zusammenarbeit mit Kunden SCC an, damit der Schutz der Daten, welche den Europäischen Währungsraum verlassen, die Grundlagen der DSGVO einhalten.[214]

Der Verantwortliche oder der Auftragsbearbeiter müssen ihre Sorgfaltspflicht wahrnehmen und bei einer, auf SCC basierenden Bekanntgabe ins Ausland sicherstellen, dass angemessene Massnahmen getroffen werden, damit garantiert werden kann, dass die Empfängerin oder der Empfänger der Daten die SCC auch tatsächlich beachtet und umsetzt.[215]

[211] EDÖB, Die Übermittlung von Personendaten, S. 2.
[212] Art. 10 Abs. 2 DSV
[213] EDÖB, Das nDSG aus Sicht des EDÖB.
[214] Microsoft, European Union Model Clauses.
[215] Art 10 Abs. 1 DSV

5.10 Zwischenfazit Bundesgesetz über den Datenschutz (nDSG)

Im nDSG wird die Bearbeitung von personenbezogenen Daten geregelt. Die datenschutzkonforme Bearbeitung basiert auf der Einhaltung der datenschutzgesetzlichen Grundsätze der Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, zweckbasiert und dass die Daten der Wahrheit entsprechen. Besteht keine gesetzliche Grundlage muss eine Einwilligung bei der betroffenen Person eingeholt werden.[216] Durch den Einsatz geeigneter TOM, wie bspw. durch eine technische Verschlüsselung, muss die Datensicherheit gewährleistet werden.[217] Der Bundesrat hat dazu Minimalanforderungen festgelegt. Die DSV präzisiert zudem, dass zur Evaluation des Schutzbedarfs der Daten ein Schutzbedarfsanalyse durchgeführt werden muss. Dabei ist gemäss Gesetzgeber das angemessene Verhältnis zwischen bestehenden Risiken und dem zu erbringendem Schutz und nicht ein absoluter Schutz zu gewährleisten.[218] Ergibt sich aus einer Datenbearbeitung ein hohes Risiko für die betroffene Person, muss eine DSFA erstellt werden. Für eine nachfolgend erfolgreiche Durchführung einer Datenbearbeitung müssen vorab die durch die DSFA evaluierten Risiken mit geeigneten TOM in einem angemessenen Mass reduziert werden.[219] Werden Personendaten durch den Verantwortlichen an einen Auftragsbearbeiter, bspw. einen Cloud-Anbieter, ausgelagert, muss die Wahl des Auftragsbearbeiter mit Sorgfalt geschehen und mit Verträgen abgesichert werden.[220] Es wurde zudem ersichtlich, dass besonders schützenswerten Daten wie Gesundheitsdaten durch das nDSG nicht differenziert betrachtet werden.[221] Ein zusätzlicher Schwierigkeitsfaktor bildet der Grad der Anonymisierung, was bspw. im Bereich der Sekundärnutzung von Gesundheitsdaten eine zentrale Frage darstellt.[222]

Die Bekanntgabe in ein Land ohne angemessenen Datenschutz ist möglich, wenn ein völkerrechtlicher Vertrag, Datenschutzklauseln oder spezifische Garantien, SCC oder verpflichtende Datenschutzvorschriften zwischen dem Verantwortlichen und dem Auftragsbearbeiter gewährleistet wird.[223]

[216] Vgl. Kap. 5.3.2; Kap. 5.3.7
[217] Vgl. Kap. 5.3.3
[218] Vgl. Kap. 5.3.4
[219] Vgl. Kap. 5.3.5
[220] Vgl. Kap. 5.3.6
[221] Vgl. Kap. 5.3.1
[222] Vgl. Kap. 5.3.7
[223] Vgl. Kap. 5.9

6 Exkurs: Rahmenwerke und gesetzliche Bestimmungen ausserhalb des nDSG

6.1 Privacy Shield und Schrems II

Im Kontext der Bekanntgabe personenbezogener Daten in die USA wurden in den vergangenen Jahren einige Rechtsprechungen erlassen und auch wieder für ungültig erklärt. Da viele grosse Cloud-Anbieter aus den USA stammen, wird diese Thematik im folgenden Abschnitt näher erläutert.

Sobald Daten ins Ausland transferiert werden, muss sichergestellt werden, dass für die Daten ein angemessener Schutz vorhanden ist.[224] Am 12. Januar 2017 wurde das «Privacy Shield»-Regime (PS-Regime) in Kraft gesetzt, welches den Datentransfer von der Schweiz in die USA unter Einhaltung der darin festgelegten Grundsätze regelt. Dabei wurde in der bestehenden Staatenliste auf das PS-Regime verwiesen und für die USA ein «partiell» angemessener Datenschutz i.S.v. Art. 6. Abs. 1 DSG festgestellt. Die Erreichung eines partiell angemessenen Datenschutzes und damit die erlaubte Durchführung von Datentransfer zwischen den USA, der EU und der Schweiz war für US-Unternehmen nur möglich mittels Absolvierens eines Zertifizierungsverfahrens. Gemäss dem Schweizer PS-Regime müssen zum einen die zertifizierten Unternehmen aus den USA die Datenschutzgrundsätze der Schweiz einhalten. Zum anderen bietet es Lösungen für Garantien im Kontext von Zugriffen durch die US-Behörden auf Personendaten, welche in die USA transferiert wurden.[225]

Am 16. Juli 2020 wurde die Angemessenheit des Schutzes, welcher durch das Privacy Shield Regime gewährleistet wird, durch den Europäischen Gerichtshof (EuGH) für ungültig erklärt.[226] Dieses Urteil ist bekannt unter dem Namen «Schrems-II-Urteil». Auf Basis der DSGVO wurden die Bearbeitungsverantwortlichen und in zweiter Instanz die Datenschutzbehörden verpflichtet, bei jedem einzelnen Datenexport die SCC auf deren Vereinbarkeit mit dem EU-Recht zu prüfen. Das Urteil ist für die Schweiz rechtlich unverbindlich, da die Schweiz nicht Teil der EU ist. Zu beachten ist jedoch, dass Schweizer Unternehmen, welche Daten gemäss Art. 3 DSGVO bearbeiten, von der Änderung betroffen sein können und sich somit an das EU-Recht halten müssen.[227] In der Schweiz sind Rechte wie der Schutz der Privatsphäre[228], allgemeine Verfahrensgarantien (Art. 29 ff. BV), die Achtung des Privat- und Familienlebens[229] sowie die Grundsätze einer

[224] EDÖB, Übermittlung ins Ausland.
[225] EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA, S. 2 f.
[226] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ltd, Maximilian Schrems, Rn. 203
[227] EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA, S. 4 f.
[228] Art. 13 BV
[229] Art. 8 EMRK

rechtmässigen, verhältnismässigen und zweckgebundenen Datenbearbeitung verankert (vgl. Kap. 5.3.2).

Der EDÖB kam in seinen Berichten zum Schluss, dass die Rechtsansprüche Schweizer Betroffener bei einem Zugriff durch US-Behörden fehlten und die Unabhängigkeit der Ombudsstelle vom US-Geheimdienst in Frage gestellt werden müsse. Da die Schweizer Grundsätze in den USA nicht vergleichbar durgesetzt werden, resultierte der EDÖB gestützt auf die Schweizer Rechtsgrundlagen, dass die USA in den Belangen der grenzüberschreitenden Bearbeitung von Personendaten keinen angemessenen Datenschutz gewährleisten kann. Hinsichtlich der SCC sowie sämtlichen ähnlichen Bestimmungen stellte der EDÖB fest, dass diese den Anforderungen an die gesetzlich vorgesehenen Garantien nicht nachkommen.[230]

Im Hinblick auf ein neues Abkommen arbeitet die Europäische Kommission zusammen mit der US-Regierung einen neuen «Trans Atlantic Data Privacy Framework» aus, in dem die Bürgerrechte geschützt werden und der transatlantische Handel für kleinere und mittlere Unternehmen ermöglicht wird.[231]

In der Zwischenzeit hat die Europäische Kommission neue Standardvertragsklauseln öffentlich gemacht. Microsoft, welches die SCC auch bereits vor dem Schrems-II-Urteil angeboten hatte (vgl. Kap 5.9.1), hat diese neuen SCC bereits auf den neusten Stand gebracht und diese in ihrem sogenannten «Data Protection Addendum» ergänzt.[232]

6.1.1 Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

Der CLOUD Act regelt im Kontext von schweren Straftaten den Zugriff auf Daten von Unternehmen mit Sitz in den USA durch US-Behörden. Das Abkommen gilt auch für Tochtergesellschaften. Das bedeutet, von Anbietern sowie Kommunikationsdiensten wird die Herausgabe von Daten verlangt, was wiederum bedeutet, dass auch Daten, welche ausserhalb der USA gespeichert sind, durch die US-Behörden verlangt werden können.[233]

Obwohl diese Bestimmung zu datenschutzrechtlichen Herausforderungen führen könnte, gibt es Stimmen, welche die Risiken der Datenherausgabe weniger hoch bewerten. Einerseits unterstehen nur Strafverfolgungen dem CLOUD Act. Damit ein Fall eröffnet werden

[230] EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA, S. 5 f.
[231] Europäische Kommission, Transatlantischer Datenschutzrahmen.
[232] Microsoft, Faktencheck.
[233] BJ, S. 46.

kann, bedarf es zusätzlich einen Gerichtsbeschluss. Die Untersuchungen zielen zudem auf «US-Personen» ab.[234]

6.2 Zwischenfazit der rechtlichen Bestimmungen ausserhalb des nDSG

Das Schrems-II-Urteil hat die Angemessenheit der SCC am 16. Juli 2020 für ungültig erklärt. Die Europäische Kommission ist zurzeit an der Ausarbeitung des «Trans Atlantic Data Privacy Framework».[235] Der CLOUD Act regelt den Zugriff von US-Behörden, welcher im Fall einer Strafverfolgung einer «US-Person» verlangt werden könnte.[236]

[234] HÜRLIMANN/STEIGER, S. 203.
[235] Vgl. Kap. 6.1
[236] Vgl. Kap. 6.1.1

II EMPIRISCHER TEIL

In der Forschung unterstützt die Wahl der Methode das Erzielen von Ergebnissen.[237] Welche Methode für eine Forschung gewählt wird, gilt es sorgfältig zu entscheiden, weil der Nutzen der Daten davon abhängt.[238] Durch einen verbalen Austausch mit einem Menschen, können Informationen über Aspekte des Lebens einholt werden.[239] Die Befragung bildet wie die Beobachtung und die Analyse von Inhalten und Texten eine Methode der Sozialwissenschaft.[240] In der vorliegenden Forschungsarbeit werden die Forschungsfrage sowie deren Teilfragen durch die analysierten Ergebnisse aus Experteninterviews beantwortet. In den folgenden Abschnitten wird die Methode erläutert und deren Wahl begründet. Anschliessend wird die Umsetzung der recherchierten Theorie dargelegt.

[237] HÄDER, S. 13.
[238] HELFFERICH, S. 875.
[239] HÄDER, S. 16.
[240] SCHOLL, S. 20.

7 Forschungsmethode Experteninterview

Befragungen können unterschiedliche Strukturen und Formen haben. Bei einer Standardbefragung sind die Fragen und Antworten bereits vordefiniert und bei einer offenen Frageform werden nur wenige ungerichtete Fragen gestellt. Das Leitfadeninterview stellt eine Mischung zwischen der standardisierten und der offenen Form der Befragung dar. Es werden zwar Fragen im Vorhinein formuliert, aber die interviewte Person hat die Möglichkeit, eine offene Antwort zu geben.[241] Die Durchführung von Leitfadeninterviews ist eine Methode, um qualitative Daten zu sammeln. Qualitative Daten werden meistens in Textform abgebildet.[242] Das Experteninterview hat zum Ziel, dass sachliche Aussagen über einen spezifischen Bereich gemacht werden können.[243]

7.1 Planung und Durchführung eines Experteninterviews mittels Leitfaden

Die methodische Planung und Durchführung eines Experteninterviews können gemäss Wassermann nach den folgenden Meilensteinen abgewickelt werden[244:]

1. Auswertung der Literatur und Dokumente
2. Auswahl der Experten
3. Aufsetzen des Leitfadens
4. Vorbereitung des Interviews
5. Durchführung des Interviews
6. Auswertung der Ergebnisse

Die Wahl Personen, welche befragt werden sollen, muss zum Ziel haben, dass brauchbare Informationen resultieren, welche einen bestimmten Bereich abdecken.[245]

Wie bereits erwähnt handelt es sich beim Leitfaden um eine Befragung, welche einem bestimmten Fokus unterliegt. Beim Aufsetzen des Leitfadens werden somit gezielte Fragen zu einem Wissensgebiet festgelegt. Dabei sollte man jedoch berücksichtigen, dass diese Fragen nicht abschliessend sind, sondern sich während dem Experteninterview abhängig von der Situation und dem Interesse der forschenden Person zusätzlichen Fragen ergeben können.[246] Als Richtlinie können ungefähr fünf Fragen formuliert werden, welche jedoch im Gespräch durch besagtes Nachfragen ergänzt werden.[247]

[241] SCHOLL, S. 61.
[242] HELFFERICH, S. 875.
[243] SCHOLL. S. 96.
[244] WASSERMANN, S. 55-61.
[245] SCHOLL, S. 69.
[246] HOPF, S. 8.
[247] SCHOLL. S 68.

Der Leitfaden ist einem Ablaufplan ähnlich. Er beinhaltet fertige Fragen, Stichworte und vor allem Fragen, welche die interviewte Person zum offenen Erzählen auffordert. Bei der Erstellung folgt man gemäss Helfferich dem Grundsatz «So offen wie möglich, so strukturiert wie nötig».[248] Bei einer solchen Ausgangslage wird von der interviewenden Person erwartet, dass sie sehr achtsam dem Gesagten der Expertin oder des Experten folgt und interpretiert, damit flexibel reagiert und kritische Rückfragen gestellt werden können. Die Thematik darf somit dem Forschenden nicht unbekannt sein.[249]

Bei einem Experteninterview werden keine persönlichen Geschichten der Expertinnen und Experten abgeholt, sondern vielmehr deren Erfahrungen zu einer bestimmten Thematik, was jedoch die Äusserung der persönlichen Meinung nicht automatisch ausschliesst. In Ihrer Rolle bauen sich Expertinnen und Experten über Ausbildungen und das Sammeln von beruflichen Erfahrungen oder auch durch das Engagement ausserhalb des beruflichen Umfelds Wissen auf. Der Ablauf eines Experteninterviews wird meistens durch mit einem Leitfaden strukturiert. Es werden weniger Fragen gestellt, welche die interviewte Person zum Erzählen auffordern, sondern die Fragen werden fokussiert formuliert und durch die Experten konkret beantwortet. Dennoch nutzen Expertinnen und Experten auch die Möglichkeit, ausführliche und narrative Antworten auf sachliche Fragen zu geben. Das Nachfragen von Zusammenhängen und Prozessen sowie konkreten Abläufen ist für ein leitfadengestütztes Experteninterview geeignet. Diese Abfrage kann durch die Nutzung von Beispielen oder der Darstellungen von Anwendungsfällen durchgeführt werden, da eine allgemeine Aussage seitens der Expertin oder des Experten meistens schwierig ist.[250]

Da bei einem Leitfadeninterview kein standardisierter Fragebogen vorliegt, wird das Interview üblicherweise aufgenommen. Die Erstellung eines Trankskripts macht für die Analyse der Ergebnisse zwar Sinn, ist jedoch nicht erforderlich.[251]

7.2 Methodische Umsetzung

Für die Umsetzung wurde der Ablauf von Wassermann (vgl. Kap 7.1) genutzt. Nach einer fundierten Literaturrecherche und der Formulierung der konkreten Forschungsfragen, war der nächste Schritt die Auswahl der Experten. Da in der vorliegenden Forschungsarbeit zwei Themenschwerpunkte zu bearbeiten waren, musste die Expertenwahl sehr

[248] HELFFERICH, S. 876.
[249] SCHOLL, S. 70.
[250] HELFFERICH, S. 887 ff.
[251] SCHOLL, S. 71.

gezielt erfolgen. Da es sich als schwierig gestaltete, Expertinnen und Experten mit sowohl technischem als auch rechtlichem Hintergrund im Bereich von Confidential Computing zu finden, wurde diese Anforderung bei der Auswahl weniger hoch gewichtet und aus beiden Bereichen Expertinnen und Experten interviewet. Insgesamt wurden sechs Experteninterviews durchgeführt.

Christoph Ernst arbeitet als Architekt von Cloud-Lösungen im Bereich Security bei Microsoft Switzerland AG. David Sturzenegger ist Produkteverantwortlicher bei Decentriq, ein Schweizer Unternehmen, welches eine Plattform anbietet, die mit Confidential Computing läuft. Diese zwei Experten konnten der Forschung, nebst vereinzelten rechtlichen Aspekten, vor allem technisches Knowhow beitragen. Für fundierte rechtliche Kenntnisse war unter anderem Matthias Eigenmann sehr hilfreich. Er ist Rechtsanwalt, hat langjährige Erfahrung im Technologierecht und setzt sich aktiv mit Confidential Computing auseinander. Zudem konnten Lucian Hunger, Rehana Harasgama sowie ein anonymer Experte für ein Interview gewonnen werden. In ihrer Funktion als Rechtsanwälte, resp. Rechtsanwältin konnten sie im Bereich Datenschutz wertvolle Erfahrungen beisteuern und das Gesetz auslegen.

Die Experteninterviews wurden basierend auf einem Leitfaden vorbereitet. Um die Experteninterviews zu strukturieren, wurden drei Themenschwerpunkte sowie entsprechende Bereiche festgelegt:

- Einschätzung aus dem beruflichen Alltag:
    - Aktuelle Themen und häufige Fragestellungen
- Rechtlicher Bereich:
    - Datenschutzkonformität und Datenbearbeitung im Kontext des nDSG
    - Praktikable Überlegungen
    - Weitere relevante rechtliche Bestimmungen
- Technologischer Bereich: Cloud-Infrastruktur und Confidential Computing
    - Möglichkeiten der Verschlüsselung, Prüfung der Integrität und Anwendungsbeispiele

Die Wahl der Schwerpunkte lässt sich insofern begründen, da abhängig von den Kenntnissen der interviewten Person der Schwerpunkt auf einen der zwei Bereiche gelegt werden konnte. Der Schwerpunkt war meistens nach der ersten Frage zu den Alltagserfahrungen bereits ersichtlich. Das Ziel war, dass die beiden Bereiche sich in gewissem Masse überschneiden. Nur so konnten die Zusammenhänge und Abläufe in einen gemeinsamen Kontext gesetzt werden, was in der Literaturrecherche in diesem Ausmass nicht möglich

war. Nicht zuletzt aus diesem Grund wurde das leitfadengestützte Experteninterview als Methode gewählt. Pro Schwerpunkt wurden zwei bis drei Fragen vorformuliert. Im Anhang[252] ist ein Beispiel eines Leitfadens vorhanden. Die Fragen wurden jedoch vor jedem Experteninterview individuell vorbereitet.

Die Experteninterviews wurden online via MS Teams durchgeführt und aufgezeichnet. Für die letzte Phase der Auswertung wurden die Gespräche transkribiert. Alle Transkripte sind im Anhang der vorliegenden Arbeit einsehbar. Die Analyse der Ergebnisse wurde im nachfolgenden Kapitel niedergeschrieben.

[252] S. Anhang «Leitfaden Experteninterview»

8 Auswertung der Ergebnisse

Für die Auswertung der Ergebnisse aus den durchgeführten Experteninterviews wurden die für den Leitfaden genutzten Themenbereiche übernommen und die Aussagen der Experten entsprechend zugeordnet. Zusätzlich wurden aus Gründen der Nachvollziehbarkeit geeignete Unterkapitel verfasst. Zu beachten ist jedoch, dass diese Unterkapital alle thematisch voneinander abhängig sind und die Abgrenzung nicht immer eingehalten werden konnte. Deswegen wurde der innovative Aspekt von Confidential Computing keinem Themenbereich zugeordnet, sondern separat aufgeführt.

8.1 Aktuelle Fragestellungen und Nachfrage auf dem Markt

Die Cloud Thematik und der Wandel von der Speicherung der eigenen Daten in «den eigenen vier Wänden» zur Speicherung in der Cloud ist real und nicht mehr aufzuhalten. Der Wandel wird jedoch begleitet durch die Frage, wie man unter den gegebenen Umständen die gesetzlichen Bestimmungen des Datenschutzes einhalten und zur gleichen Zeit Vertrauen gegenüber Nutzenden aufbaut, da der Aspekt des Vertrauens ein zentraler Punkt ist.[253] Es lässt sich daraus schliessen, dass die Nachfrage nach Cloud-Migrationen sehr hoch ist. Die wird durch weitere Aussagen der Expertinnen und Experten bestätigt. Zurzeit werden häufig Projekte begleitet und beraten, welche Fragestellungen zur Cloud-Migration im Bereich des Berufs- oder Amtsgeheimnisses beinhalten.[254] Zu beachten ist dabei, dass Bereiche, welche sich unter einer speziellen Regulierung befinden, wie bspw. das Arztgeheimnis oder das Bankkundengeheimnis gegen über dem Datenschutzgesetz Vorrang haben.[255] Hingegen besteht im Bereich von Confidential Computing zurzeit noch keine grosse Nachfrage. Dazu sagte Ernst, dass er noch mit keinem Kunden Confidential Computing produktiv einsetzt. Der Einsatz dieser Technologie stellt sich als eher komplex heraus und die Expertise und Erfahrungen finden noch keine grosse Verbreitung. Zudem kann eine Anwendung, welche Bearbeitungen mittels Confidential Computing schützt, einen hohen finanziellen Aufwand erzeugen.[256]

[253] Transkript 1, Ernst, RN 1.
[254] Transkript 3, Hunger, RN 2.
[255] Transkript 5, Harasgama, RN 1.
[256] Transkript 1, Ernst, RN 7.

8.2 Rechtlicher Bereich

8.2.1 Datenbearbeitung in der Cloud

Die Experten berichteten von ihren Erfahrungen mit Cloud-Projekten und was für eine Auslagerung beachtet werden muss. Im Kontext einer Auslagerung in eine Cloud wird Klientinnen und Klienten jeweils empfohlen, beim potenziellen Auftragsbearbeiter eine Due Diligence durchzuführen. Das wird meistens unterschätzt, da es einfacher klingt, als es ist. In der Beurteilung werden auch die technischen und organisatorischen Massnahmen rechtlich geprüft. «Zu beachten ist in diesem Zusammenhang, dass Cloud-Provider oftmals auch Sub-Processors unter Vertrag haben. Da liegt genau das Risiko des Outsourcings. Man gibt die Kontrolle ab.» Danach gilt es, die Art der Daten und Form deren Auslagerung zu bestimmen. Dabei muss das Vorhandensein von spezifischen gesetzlichen Grundlagen sowie Kundenverträgen geprüft werden. Sofern die Daten ins Ausland ausgelagert werden, muss ein Transfer Impact Data Assessement durchgeführt werden. «Man geht vertraglich mehr Pflichten ein wie früher. Die Pflichten sind jedoch mittlerweile organisatorisch mit den Standard Contractual Clauses (SCC) sehr gut abgedeckt.» Microsoft bietet in der Rolle als Processor bereits standardmässig eine Auftragsdatenvereinbarung sowie SCC an.[257] Das grundsätzliche Risiko besteht insofern meistens nicht bei der Datenbearbeitung, wenn diese bereits datenschutzkonform umgesetzt wird. Es besteht ein zusätzliches Risiko in der Migration in die Cloud. Durch eine vollumfängliche rechtliche sowie technische Beurteilung und das Durchführen von Assessements kann das Risiko evaluiert werden.[258] Die Cloud-Nutzung bietet viel Kapazität und auch eine hohe Datensicherheit. Aber als Auftraggeber, bzw. Verantwortlicher müssen auch entsprechenden Kontrollen durchgeführt werden, was man vorher im Serverraum durchführen konnte. Heutzutage wird die Kontrolle über die Überprüfung eines SOC-Berichts durchgeführt und einem Dritten vertraut.[259]

Betrachtet man das Angebot auf dem Markt, stammen Cloud-Anbieter mit hohen Sicherheitsstandards aus den USA. Die amerikanischen Anbieter bieten aufgrund ihrer Erfahrungen gute Voraussetzungen in punkto Datensicherheit. In dieser Hinsicht fehlt es den europäischen und Schweizer Anbieter noch an Erfahrung.[260]

[257] Transkript 5, Harasgama RN 6.
[258] Transkript 4, Hunger, RN 2.
[259] Transkript 4, Hunger, RN 10.
[260] Transkript 5, Harasgama, RN 3.

8.2.2 Privacy Shield und Schrems II

Durch das Schrems-II-Urteil des EuGH wurde der Angemessenheitsbeschluss der SCC mit einem Drittstaat ohne angemessenen Datenschutz für ungültig erklärt. Zusätzlich muss nun auch ein Transfer Impact Assessement (TIA) durchgeführt werden. Reichen gemäss den Ergebnissen aus dem TIA die SCC für eine sichere Übermittlung nicht aus, müssen für einen angemessenen Schutz zusätzliche Massnahmen definiert werden. Vor dem Schrems II-Urteil war es im Rahmen des Privacy Shields möglich, Daten in ein Drittland zu übermitteln, wenn der Empfänger eine entsprechende Zertifizierung hatte. Das Privacy Shield Framework ist zurzeit in Überarbeitung. Aber das eigentliche Problem kann durch kein Framework gelöst werden. «Die Ausgangs-These, dass man diese SCC vereinbaren kann und anschliessend abgesichert ist, war wohl von Anfang an falsch. Man muss trotzdem stets überprüfen, ob nach diesem SCC gelebt und das auch umgesetzt werden kann.»[261] Werden die Daten nun in ein Land übermittelt, welches, verglichen zum europäischen Standard, ungenügende rechtliche Bestimmungen hinsichtlich des Handlungsspielraums von Geheimdiensten hat, muss sich ein Anbieter als Empfänger von Personendaten in den USA entscheiden zwischen der Verletzung der SCC und einer Konfrontation mit dem Geheimdienst. In einem solchen Fall liegt es gemäss EuGH nahe, dass die SCC verletzt werden. «Die Durchsetzbarkeit der SCC ist somit in Frage gestellt. Dort liegt das eigentliche Problem.» In diesem Kontext wird auch ein Ansatz genutzt, welcher berechnet, wie hoch die Wahrscheinlichkeit ist, dass der Empfänger der Daten in die vorhin erläuterte Situation mit dem Geheimdienst gerät. Mittels dieses risikobasierten Ansatzes von David Rosenthal wird in einem Impact Assessement unter anderen überprüft, ob der Geheimdienst Interesse an den Daten hegen könnte. Oftmals ergibt sich aus den Resultaten, dass das berechnete Risiko sehr klein ist.[262]

Das ist jedoch nur die eine Seite der SCC. Durch Abschliessen der SCC wird versucht, die Lücken in den Rechtsgrundlagen des Empfängerstaates vertraglich zu schliessen, damit die Grundrechte der betroffenen Person geschützt werden. Der Schutz, welcher durch ein SCC vereinbart wird, ist dem Schutz, welcher das Privacy Shield Framework und eine Zertifizierung gewährleisten, sehr ähnlich. «Es geht teilweise sogar noch weiter und ermöglicht teilweise noch einen effektiveren Schutz der betroffenen Personen, was ja das Kernanliegen des Datenschutzes ist.»[263]

[261] Transkript 3, Eigenmann, RN 5 f.
[262] Transkript 3, Eigenmann, RN 7 f.
[263] Transkript 3, Eigenmann, RN 9.

Die jeweilige Auslegung der Gesetzgebungen ist von grosser Relevanz. So könnte eine strikte Auslegung des Schrems-II-Urteils bedeuten, dass keine personenbezogenen Daten auf einer Cloud bearbeitet werden dürfen. Dies war gemäss Eigenmann womöglich nicht die Absicht des Gesetzgebers.[264]

Eine andere Auslegung des Schrems II-Urteils könnte beinhalten, dass die Übermittlung von Personendaten in Drittstaaten mittels SCC inklusive zusätzlichen technischen Massnahmen (bspw. Schlüssel für Entschlüsselung nicht im Drittland), welche den Datenzugriff technisch unmöglich machen, erlaubt ist. In der Praxis würde das bedeuten, dass eine reine Datenspeicherung erlaubt und alle weiteren Anwendungsfälle ausgeschlossen wären.[265] Mittels einer solchen Verschlüsselung hat man einerseits das Vertrauensproblem gelöst, da das Drittland nicht auf die Daten zugreifen kann. Im Gegenzug können jedoch die Dienstleistungen einer Cloud nur in beschränktem Masse genutzt werden, da die Daten in der Cloud nicht bearbeitet werden können. Genau an diesem Punkt setzt Confidential Computing an.[266]

«Selbst wenn man von einer strengst möglichen und restriktiven Auslegung von Schrems II ausgeht, müsste Confidential Computing die Datenübermittlung in die USA und andere Staaten ermöglichen, vorausgesetzt, dass es entsprechend aufgegleist ist, und dass, wie bereits erwähnt, die Kontrolle über den Schlüssel ausserhalb dieser Staaten bleibt.»[267]

Man muss berücksichtigen, dass Vertrauen und Datensicherheit durch einen Vertrag nicht automatisch herbeigeführt werden. Trotzdem erhofft man sich den Aufbau von mehr Vertrauen durch die Ausarbeitung des Trans Atlantic Data Protection Framework.[268]

8.3 Technologischer Bereich

8.3.1 Cloud-Infrastruktur, Verschlüsselung und Datenzustände

Ein Cloud-Provider baut die Dienstleistungen gemäss dem «Shared Responsability-Modell» auf. «Unabhängig welche Dienstleistungen man bei einem Cloud-Anbieter beansprucht, bleibt der Provider verantwortlich für die Sicherheit der Cloud («Security of the Cloud»). Der Kunde bleibt immer in der Verantwortung der provisionierten Services, welche beansprucht werden («Security in the Cloud»)».[269]

[264] Transkript 3, Eigenmann, RN 3.
[265] Transkript 3, Eigenmann, RN 7.
[266] Transkript 3, Eigenmann, RN 4.
[267] Transkript 3, Eigenmann, RN 10.
[268] Transkript 6, RN 11.
[269] Transkript 1, Ernst, RN 2.

Möchte man personenbezogenen Daten und insbesondere besonders schützenswerte Daten in einer Cloud speichern, ist zu empfehlen, einen Anbieter zu wählen, der die Regulierungen einhält und Standards bietet. Die Infrastruktur sollte laufend Prüfungen unterzogen werden. Es gilt zudem, den Zugriff, die Speicherung und die Verwendung der Verschlüsselung den Vorgaben entsprechend zu klären.[270]

Hat man eine reine Datenspeicherung in einer Cloud und der Cloud-Anbieter hat keinen Zugriff auf den Schlüssel, muss man zwar kein Vertrauen gegenüber dem Cloud-Anbieter aufbauen, da kein Zugriff möglich ist, dennoch verunmöglicht dieser Umstand die Nutzung von weiteren Cloud-Dienstleistungen nebst der reinen Speicherung.[271]

Da sich vielen Unternehmen keine interne IT-Sicherheitsabteilung leisten können, lässt sich in diesen Fällen die Nutzung einer Cloud als sicherer einstufen. Generell liegt die Cloud im Trend und Confidential Computing gewährleistet in diesem Kontext einen noch höheren Schutz.[272] Es ist jedoch Tatsache, dass momentan eher noch zurückhaltend mit besonders schützenswerten Daten in der Cloud gearbeitet wird, da es womöglich zurzeit noch ein zu grosses Risiko mit sich bringt.[273]

Technisch gilt es nachzuvollziehen, dass es drei unterschiedliche Zustände von Daten gibt. Gespeicherte Daten («Data at Rest») und Daten während der Übertragung («Data in Transit») können heutzutage sehr sicher verschlüsselt werden. Diese Art von Verschlüsselung kann für Daten in Bearbeitung («Data in Use») nicht entsprechend gewährleistet werden. «Confidential Computing schliesst diese Lücke.»[274]

Confidential Computing wird als hardware-basierte Technologie in Form von Chips bereits seit längerem bspw. in Handys eingesetzt. Der Umstand, dass Hyperscalers wie Google und Microsoft in den vergangenen Jahren das Anbieten von Confidential Computing-Lösungen auf Servern in ihren Rechenzentren starteten, ergab die Schnittstelle zur Cloud.[275]

Es gibt unterschiedliche Anwendungsfälle von Confidential Computing, wobei ein Anwendungsfall die Durchführung von Datenkollaborationen ist. Eine konventionelle Lösung beinhaltet den Austausch, resp. die Freigabe der Daten zwischen zwei Parteien oder zusätzlich einer Drittpartei, was oftmals aus Datenschutzgründen nicht gewollt oder erlaubt ist. Decentriq hat dafür, gestützt auf die Confidential Computing-Technologie, eine

[270] Transkript 1, Ernst, RN 4.
[271] Transkript 3, Eigenmann, RN 4.
[272] Transkript 2, Sturzenegger, RN 6.
[273] Transkript 1, Ernst, RN 9.
[274] Transkript 1, Ernst, RN 6.
[275] Transkript 3, Eigenmann, RN 2.

Plattform gebaut. Die Daten werden in Datenräumen mittels eines Codes berechnet und in anonymen Zustand herausgegeben. Keine Partei kann in diesem Datenraum auf die Daten zugreifen oder die Berechnungen mutieren.[276]

Hinsichtlich des Zugriffs muss man jedoch anmerken, dass für eine Technologie nie eine hundertprozentige Sicherheit gewährleistet werden kann. Technologien bieten Raum für Schwachstellen und es gilt auch, die Parteien in der Vertrauenskette, in vorliegenden Kontext Intel, zu berücksichtigen. Risiken gibt es immer und diese gilt es von Fall zu Fall abzuwägen. Confidential Computing wurde jedoch für sämtliche Praxisgründe «als sehr sicher eingestuft».[277]

Ein weiteres Restrisiko kann bspw. auch durch eine falsche Nutzung bestehen. Um dieses «menschliche Versagen» zu minimieren, hat Decentriq bereits ein Feature eingebaut, welches den Input und den Output zu Gunsten der Privatsphäre regelt.[278] Das Ergebnis der Berechnungen wird in einer Form herausgegeben, in der eine Re-Identifizierung der betroffenen Personen nicht möglich ist.[279]

8.3.2 Prüfung der Integrität von Confidential Computing

Confidential Computing gewährleistet zwei Sicherheitsaspekte. Es handelt sich zum einen um die sogenannte «Encryption in Use», was die Datenspeicherung im Arbeitsspeicher beinhaltet. Das verhindert den Zugriff oder das Herunterladen von Daten aus dem Arbeitsspeicher. Der zweite Aspekt ist die «Remote Attestation», welche der Endnutzerin und dem Endnutzer die Integrität der Confidential Computing-Plattform bestätigt (Daten werden mittels eines bestimmten Codes in einer Confidential Computing-Infrastruktur berechnet). Die Zusammenarbeit basiert mit Vorhandensein dieses Aspekts nicht auf blossem Vertrauen gegenüber dem Anbieter.[280]

Bei grösseren Unternehmen wird die Prüfung oftmals über das Einholen von SOC-2-Berichten, entsprechende Zertifizierungen und externen Auditberichten durchgeführt. Natürlich müssen intern auch Kompetenzen vorhanden sein und weitere Überprüfungen stattfinden. Ein Bericht bedeutet nicht automatisch, dass etwa geprüft ist.[281]

Externe Auditberichte sind teilweise jedoch schwierig in der Durchsetzung. Es bleibt wohl dabei, dass man Vertrauen in den Anbieter haben muss. Aufsichtsbehörden könnten

[276] Transkript 2, Sturzenegger, RN 1 f.
[277] Transkript 2, Sturzenegger, RN 4.
[278] Transkript 2, Sturzenegger, RN 9 f.
[279] Transkript 3, Eigenmann, RN 18.
[280] Transkript 2, Sturzenegger, RN 7.
[281] Transkript 4, Hunger, RN 8.

anhand von Richtlinien und Empfehlungen das Vertrauen aufbauen. Es geht nicht darum, mittzuteilen, was man nicht darf, sondern vielmehr darum, Guidelines zu sprechen, welche aufzeigen, was erlaubt ist.[282]

Optimal ist, wenn eine interne IT-Abteilung existiert, welche solche Beurteilungen durchführen kann. Als Standard gilt, dass man alles dokumentiert hat und nachweisen kann, dass eine Datenbearbeitung entsprechend den rechtlichen Anforderungen ausgestaltet wird. Bei komplexeren Themen sollte das Verständnis soweit vorhanden sein, dass eine realistische Beurteilung durchgeführt werden kann.[283]

8.4 Was ändert sich durch den Einsatz von Confidential Computing?

Wird berücksichtigt, was über die technischen Massnahmen im Kontext von Schrems II bereits verschriftlicht wurde, müsste bei einer Analyse von Daten in einer Umgebung, welche durch Confidential Computing betrieben wird und somit technisch verschlüsselt ist, der Standort des Servers ausgeklammert werden. Wenn diese Ausgangslage zukünftig juristisch begutachtet werden würde, «würde sich eine rechtliche Erhebung des Serverstandortes erübrigen».[284]

Mit Confidential Computing lassen sich technisch die Risiken des Datenzugriffs sowie der Datensicherheit lösen, resp. minimieren. Daraus lässt sich schliessen, dass Confidential Computing auch einen Lösungsansatz hinsichtlich der Unsicherheit der Cloud mit sich bringt. Die Umgebung von Confidential Computing ist technisch isoliert, sodass kein Zugriff mehr möglich ist.[285]

Dennoch wird argumentiert, dass man abwägen muss, ob der Einsatz von Confidential Computing für die Erfüllung des Schutzbedarfs der Daten notwendig ist. Eine Cloud muss auf einem stabilen Fundament aufgebaut sein. Dabei spielen «Security Best Practices und eine sichere Verschlüsslungsstruktur eine zentrale Rolle.» Der Schlüssel soll dabei durch die Nutzerin oder den Nutzer kontrolliert und sicher im System gespeichert werden. Die Sicherheit des Systems kann durch Zertifizierungen garantiert werden. Ein weiterer zentraler Punkt stellt der Ort des Servers dar. Nutzerinnen und Nutzer können im Fall von Microsoft selbst wählen, an welchem Standort die Daten gespeichert werden sollen, was im Kontext von besonders schützenswerten Daten einen hohen Stellenwert geniesst. Durch Reports und Compliance-Standards können zudem Fragen hinsichtlich des

[282] Transkript 5, Harasgama, RN 12.
[283] Transkript 6, RN 9.
[284] Transkript 3, Eigenmann, RN 4.
[285] Transkript 6, RN 10.

Schutzes von Daten in Bearbeitung beantwortet werden. Es resultiert daraus, dass ein Grossteil der notwendigen Schutzmassnahmen somit bereits ohne den Einsatz von Confidential Computing umgesetzt werden können, was das Engagement von Cloud-Anbietern im Bereich der Datensicherheit aufzeigt.[286]

Eigenmann führt diesen Aspekt folgendermassen aus: Damit die Dienstleistungen einer Cloud ausgeführt werden können, muss dem System Zugriff auf die Daten gewährt werden. In der Regel besitzen Administratoren entsprechende Berechtigungen, welche den Zugriff auf die Daten ermöglichen. Bestenfalls unterliegt die Zusammenarbeit zwischen den Nutzenden und dem Cloud-Anbieter vertraglichen Bestimmungen, welche den Zugriff einschränken. Dann gibt es auch organisatorische Massnahmen seitens des Anbieters, welche den Zugriff auf Klartexte nur mittels Vier-Augen-Prinzip gewähren. Die Tatsache, dass die Wahl der zweiten Person per Zufallsprinzip gewählt wird, erschwert die Angriffe mit böswilligen Absichten zusätzlich. Aber auch durch das Einsetzen vorher genannter Massnahmen besteht weiterhin das Risiko, dass ein sogenannter «Super-Administrator» auf die Daten zugreifen kann, was sich Cloud-Anbieter auch bewusst sind. Es wird in diesem Bereich sehr viel unternommen, um Vertrauen zu schaffen.[287]

Das dargelegte Risiko, welches sich durch den Zugriff der Administratoren ergibt, wird durch die Nutzung von Confidential Computing eliminiert. Es wird eine organisatorische Massnahme durch eine technische Massnahme ersetzt, bei der man nicht mehr in den Administrator, sondern in die Technologie vertrauen muss.[288] Die Angemessenheit der technischen und organisatorischen Massnahmen (TOM) sind bei einer Datenbearbeitung zentral. Dabei muss der Schutzbedarf der Daten berücksichtigen werden, was mit der Abwägung von Risiken zusammenhängt. Die Risiken sollen dann mittels TOM minimiert werden. Confidential Computing ermöglicht den zusätzlichen Schutz der Daten in Bearbeitung (Data in Use). «Das heisst, die technische Schutzmassnahme von Confidential Computing bietet plötzlich einen Schutz, welcher durch traditionelle Verschlüsselungsmethoden nicht gewährleistet werden konnte.» Die Angemessenheit der Schutzmassnahmen lässt sich aufgrund des höheren Schutzstandards eher rechtfertigen.[289] Mittels der technischen Möglichkeit der Verschlüsselung wird Vertraulichkeit der Daten «in erhöhtem Mass» sichergestellt.[290]

[286] Transkript 1, Ernst, RN 7 f.
[287] Transkript 3, Eigenmann, RN 11 ff.
[288] Transkript 3, Eigenmann, RN 14.
[289] Transkript 3, Eigenmann, RN 17.
[290] Transkript 3, Eigenmann, RN 11.

Die Tatsache, dass die Daten aus dem Datenraum in anonymer Form herausgegeben werden, eliminiert das Risiko der betroffenen Person fast gänzlich.[291]
Aus rechtlicher Perspektive ist stets der Zweck der Datenbearbeitung von grosser Bedeutung für die Datenschutzkonformität.[292] Mittels Confidential Computing kann der Code für die Berechnungen genau definiert und somit der Zweck der Datenbearbeitung sehr detailliert bestimmt werden.[293]
Es ist zu vermuten, dass Confidential Computing zurzeit noch zu unbekannt ist und deswegen noch nicht viele juristische Meinungen bestehen. Dieser Umstand dürfte sich mit der Nennung von konkreten Anwendungsfällen ändern. Im Kontext der USA wird stets erwähnt, dass es keine vertragliche Lösung gibt und es wird festgestellt, dass dies technisch gelöst werden muss.[294]

8.4.1 Anwendungsbeispiele

Aus den Gesprächen wurde ersichtlich, dass Confidential Computing in der Marketing- sowie in der Gesundheitsbranche, unter anderem durch die Nennung konkreter Beispiele, Nutzungspotenzial aufweist.

Marketingbranche: In der Marketingbranche sehen die Expertinnen und Experten grosses Potenzial in der Nutzung von Confidential Computing. Dabei geht es um die Frage, wie die Daten von Kundinnen und Kunden genutzt werden können, ohne deren Privatsphäre zu verletzen.[295]
In den isolierten Datenräumen, welche unter Confidential Computing laufen, werden die Berechnungen der Daten ohne Personenbezug ausgeführt. Der Zugriff wird technisch verunmöglicht. Nebst der Bearbeitung von sensiblen Daten könnten somit auch Bearbeitungen erfolgen, welche zuvor einen anderen Zweck hatten. Die theoretische Pseudonymisierung kann gemäss neuem Urteil als Anonymisierung betrachtet werden. In dieser Hinsicht könnte Confidential Computing somit von Nutzen sein. Man führt einerseits eine Datenbearbeitung durch, welche nicht sehr «nutzerfreundlich» ist, aber die Bearbeitung wird durch eine Technologie dennoch gesetzeskonform. In diesem Bereich besteht Entwicklungspotenzial.[296]

[291] Transkript 2, Sturzenegger, RN 3.
[292] Transkript 4, Hunger, RN 10; Transkript 3, Eigenmann, RN 18.
[293] Transkript 3, Eigenmann, RN 18.
[294] Transkript 5, Harasgama, RN 10.
[295] Transkript 2, Sturzenegger, RN 2.
[296] Transkript 6, RN 7.

Beispiel Marketing:

- Die Nutzung der «First Party Data» in «Data Clean Rooms» ist zurzeit sehr gefragt. Ein Unternehmen kann zur Werbeoptimierung interne Daten mit den Daten eines Dritten abgleichen und aus dem Ergebnis evaluieren, wie Werbung effizient eingesetzt werden kann. Der Kontext für dieses Aufkommen ist die baldige Abschaffung der «Third Party Cookies», welche das Verfolgen der Nutzerinnen und Nutzer über mehrere Webseiten verunmöglicht.[297]

Gesundheitsbranche: Bei Gesundheitsdaten spielt in punkto Datensicherheit die Vertraulichkeit eine sehr zentrale Rolle.[298] Diese gilt es sicherzustellen. «Noch wichtiger ist, dass ein Spital die Kontrolle über die Daten behält.» Diese unterschiedlichen Ansätze von Confidential Computing, welche dies sicherstellen, muss man rechtlich begutachten.[299]
Im Bereich der Sekundärnutzung in der Forschung könnte Confidential Computing Vertrauen schaffen. Es könnte Möglichkeiten in der Nutzung eröffnen, welche durch die bisher verfügbare Technologie nicht vorhanden waren.[300] Zu berücksichtigen ist jedoch, dass im Gesundheitsbereich bereits sehr strikte Vorgaben, bspw. durch das Humanforschungsgesetz, bestehen.[301]
Fakt ist, dass die Sekundärnutzung in der Schweiz aufgrund der komplexen Gesetzgebung fast nicht möglich ist, da es für Entscheidungsträger kaum realisierbar ist, eine angemessene Beurteilung der rechtlichen Risiken durchzuführen. Diese Tatsache wurde in einem Gutachten[302] von Meyerlustenberger Lachenal kürzlich publiziert. Dabei wurde aber auch angedeutet, dass durch den Einsatz von Confidential Computing in der Schweiz gewisse Probleme in der Sekundärnutzung von Gesundheitsdaten lösbar sein könnten. Inwiefern die Risiken, welche im Gutachten erwähnt wurden, mittels Confidential Computing minimiert werden können, müsste in einem nächsten Schritt rechtlich evaluiert werden.[303]

[297] Transkript 2, Sturzenegger, RN 2.
[298] Transkript 3, Eigenmann, RN 16.
[299] Transkript 3, Eigenmann, RN 21.
[300] Transkript 6, RN 4.
[301] Transkript 6, RN 2.
[302] Details unter: https://www.interpharma.ch/wp-content/uploads/2022/10/Gutachten-Interpharma_Sekundaernutzung-Gesundheitsdaten.pdf
[303] Transkript 3, Eigenmann, RN 21.

Beispiele Gesundheitsbranche:

- In den USA wird Confidential Computing in der Zusammenarbeit zwischen unterschiedlichen Gesundheitsinstitutionen genutzt. Diese Institutionen liefern private Gesundheitsdaten, welche für das Training einer künstlichen Intelligenz genutzt werden. Dabei haben die einzelnen Institutionen lediglich Zugriff auf ihre eigenen Daten.[304]
- Im Bereich der Datenkollaborationen führt Decentriq eine Kollaboration mit Roche. Roche hat ein sensitives Modell entwickelt, welches den Krankheitszustand einer Person in Erfahrung bringen soll. Damit das Modell auf seine Eignung geprüft werden kann, werden spezifische Daten aus einem Spital, welche besonders schützenswert sind, in das Modell eingespeist.[305]

[304] Transkript 1, Ernst, RN 3.
[305] Transkript 2, Sturzenegger, RN 2.

III DISKUSSION

9 Beantwortung der Forschungsfragen

a) Was ist der Unterschied zwischen Trusted Computing und Confidential Computing?

In Kap. 2 wurde das Thema Trusted Computing und in Kap. 4 das Thema Confidential Computing ausführlich bearbeitet. In der Tabelle 1 werden diese zwei Technologien auf Basis ihrer Eigenschaften und ihrer Funktion übersichtlich gegenübergestellt. Es wird ersichtlich, dass diese beiden Technologien Hardware-basiert sind und eine erhöhte Sicherheit innerhalb eines Systems gewährleisten. Der Fokus bei der Wahrung der Integrität unterscheidet sich jedoch und beide Technologien setzen an unterschiedlichen Punkten an. Während Trusted Computing den Fokus auf der Vertrauenswürdigkeit der Plattform selbst und bei der Datenspeicherung hat, setzt Confidential Computing bei der Vertraulichkeit der Datenbearbeitung an. Es gilt nicht entweder oder sondern es handelt sich bei Trusted Computing und Confidential Computing viel mehr um komplementäre Technologien, die zusammen zu einem erhöhten Sicherheitsniveau einer Plattform beitragen.

Tabelle: 1: Vergleich von Trusted Computing und Confidential Computing

	Trusted Computing	**Confidential Computing**
Basis	Passiver Hardware Chip, Trusted Platform Module (TPM)	Aktiver Hardware Chip, Trusted Execution Environment (TEE)
Anwendungsfälle und Sicherheitsprinzipien	• Sichere Speicherung von Benutzerdaten, Zertifikaten und Schlüsselmaterial für Verschlüsselung (Data at Rest). • Vertrauenskette: Alle Komponenten sind über durch einen vertrauenswürdigen Pfad verbunden • Integritätsprüfung durch «Remote Attestation»: erlaubt sichere	• Datenbearbeitung (Data in Use) in isolierter Enklave, geschützter Datenraum für alle sensiblen und schützenswerten Daten. Zugriff durch unberechtigte ausgeschlossen. • «Encryption in Use»: Zugriff, Veränderung und Herunterladen von Daten im Arbeitsspeicher unmöglich.

	Übermittelung von sensiblen Daten an einen externen Server. • Plattform Authentifizierung: Sicherstellung eines vertrauenswürdigen Computersystems, z.B. in einer VPN-Umgebung.	• Sealing-Funktion: Verschlüsselte Datenspeicherung auf der Festplatte nach der Datenbearbeitung. • «Remote Attestation»: Integritätsprüfung, Verifizierung der CC-Umgebung und des Codes, durch welchen die Berechnungen durchgeführt werden. • TEE kann Sicherheitsstandards der Programmcodes erkennen und entsprechend ausführen. Schutz von gesamten unkontrolliertem Benutzercode. Zugriff bzw. Mutation der Daten oder des Codes technisch unterbunden.
Limitierung	Kein Schutz vor Zugriff auf unverschlüsselte Daten, die gerade in Bearbeitung sind.	Keine Prüfung und Sicherstellung einer vertrauenswürdigen Plattform, hingegen wird die Confidential Computing-Umgebung selbst validiert.
Aktuelle Nutzung	Heutzutage standardmässig in Geräten (Computer, Smartphones etc.) vorhanden und verwendet.	Isolierte Enklaven (TEE) werden heute bereits in Smartphones verwendet, im Bereich von Datenkollaborationen im Marketing, Gesundheitswesen und allgemein in der Forschung jedoch erst in der Anfangsphase (Thematik wird ausführlicher in Frage b) erläutert).

b) Wie muss gemäss dem neuen Datenschutzgesetz vorgegangen werden, damit eine Datenbearbeitung datenschutzkonform umgesetzt wird?

Die Forschungsfrage wird basierend aus den Erkenntnissen aus Kap. 5 und Kap. 6, sowie ergänzend durch die Ergebnisse aus den Experteninterviews beantwortet. Die Tabelle 2 zeigt die rechtlichen Grundlagen einer datenschutzkonformen Datenbearbeitung und was hinsichtlich der Datensicherheit eingehalten werden muss. Unternehmensinterne strukturelle Vorgaben aus dem nDSG und die Konsequenzen und Handlungsanweisungen einer Datenschutzverletzung bleiben aus Gründen der Relevanz unbeleuchtet.

Tabelle: 2: Datenschutzkonforme Datenbearbeitung gemäss nDSG

<table>
<tr><th colspan="3">Anforderungen aus dem nDSG</th><th>Bemerkungen / Expertenmeinungen</th></tr>
<tr><td colspan="3">Grundsätze Datenschutz</td><td></td></tr>
<tr><td>Gesetzliche Grundlage</td><td>oder</td><td>Einwilligung</td><td><u>Zu beachten</u>: lex specialis wie bspw. Berufsgeheimnis (Art. 321 StGB), Humanforschungsgesetz (HFG); Einwilligung muss freiwillig nach angemessener Information erfolgen Art. 6 Abs. 6 nDSG;</td></tr>
<tr><td colspan="3">Prinzipien der Datenbearbeitung (Art. 6 nDSG)</td><td></td></tr>
<tr><td colspan="3">Rechtmässigkeit (Art. 6 Abs. 1 nDSG)
Treu und Glauben und Verhältnismässigkeit (Art. 6 Abs. 1 nDSG)
Zweck (Art. 6 Abs. 3 nDSG)
Richtigkeit (Art. 6 Abs. 5 nDSG)</td><td><u>Zweck</u>: Bearbeitung findet zu einem bestimmten Zweck statt. Die Daten werden nur gemäss diesem Zweck beschafft. Sobald der Zweck der Datenbearbeitung obsolet ist, erfolgt die Vernichtung oder Anonymisierung der Personendaten. Ein spannender Punkt in diesem Kontext ist die mögliche Zweckerweiterung in der Sekundärnutzung.

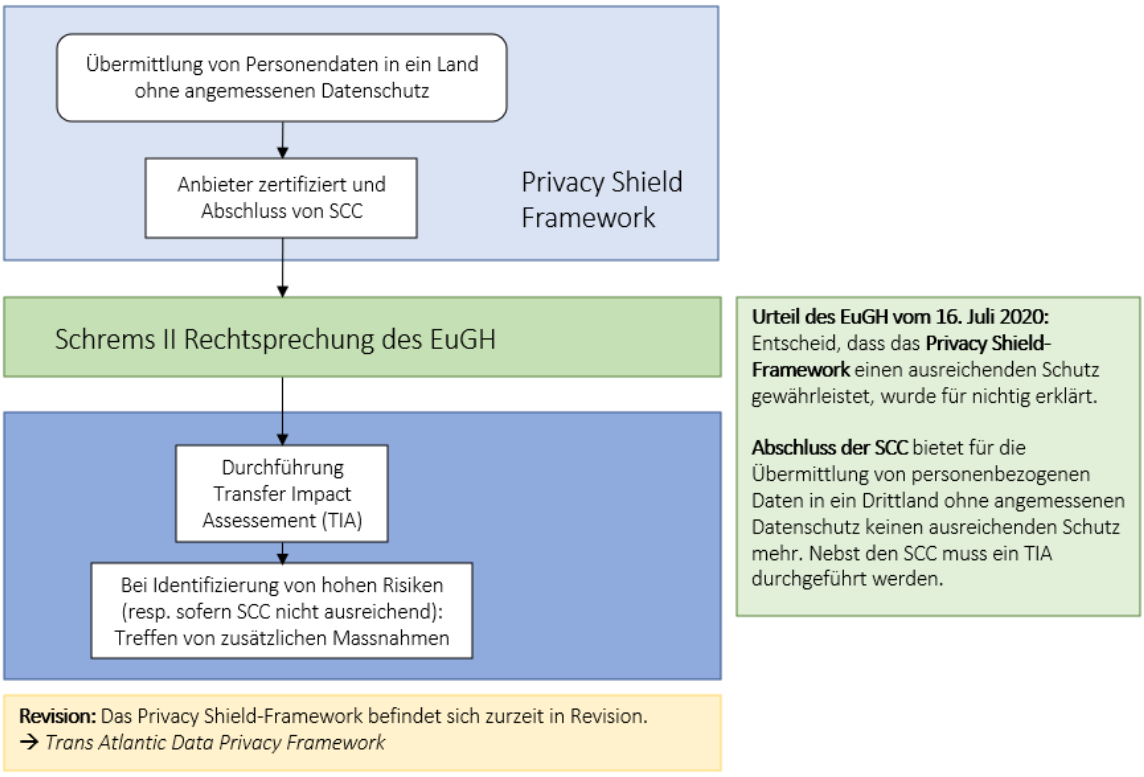
Durch den Einsatz von TOM müssen die Grundsätze eingehalten werden.</td></tr>
<tr><td colspan="4">Datenschutz durch technische und organisatorische Massnahmen (TOM, Art. 7 nDSG)</td></tr>
<tr><td>Technische Massnahmen</td><td colspan="2">Organisatorische Massnahmen</td><td rowspan="2">Damit Datensicherheit gemäss Art. 8 nDSG gewährleistet werden kann, müssen den Risiken entsprechend angemessene TOM getroffen werden (Risikoanalyse), damit Datenschutzverletzungen vermieden werden können.
Damit die Risiken evaluiert und angemessene TOM getroffen werden können, muss gemäss DSV eine Schutzbedarfsanalyse durchgeführt werden (Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit, Art. 2 DSV)</td></tr>
<tr><td>Angemessener technischer Schutz der Personendaten vor Risiken
Bsp. Verschlüsselung</td><td colspan="2">Angemessene organisatorische Gestaltung datenschutzfreundlicher Voreinstellungen
Bsp. Verwaltung der Berechtigungen (Zugriff, Zutritt)</td></tr>
<tr><td colspan="4">Minimalanforderungen an die Datensicherheit (Art. 1 DSV)</td></tr>
<tr><td colspan="2">Durchführung einer Schutzbedarfsanalyse</td><td rowspan="2">Art der bearbeiteten Daten: Bsp.: Sind es besonders schützenswerte Daten?
<u>Zu beachten</u>: Das Gesetz verlangt keinen absoluten Schutz, sondern vielmehr das Abwägen von Risiken und potenziellen Schutzmassnahmen zur Eliminierung, bzw. Reduzierung der Risiken. Werden Risiken eingegangen ist ein (gesetzliches) Argumentarium notwendig.</td></tr>
<tr><td>Art der bearbeiteten Daten (Art. 1 Abs 2 lit. a DSV)</td><td>Zweck, Art, Umfang, Umstände der Bearbeitung (Art. 1 Abs. 2 lit. b DSV)</td></tr>
</table>

<table>
<tr><th colspan="2">Anforderungen aus dem nDSG</th><th>Ergänzungen / Expertenmeinungen</th></tr>
<tr><td colspan="3">Datenschutz-Folgenabschätzung (DSFA, Art. 22 nDSG, Art. 23 nDSG)</td></tr>
<tr><td>Datenbearbeitung verursacht keine hohen Risiken</td><td>Keine DSFA nötig; Risiken können mittels angemessenen TOM bereits minimiert werden</td><td rowspan="2">Zu beachten: Die Durchführung einer DSFA ist den Prinzipien des «Privacy by Design» ähnlich. Die Durchführung einer DSFA kann somit die Umsetzung der technischen Massnahmen unterstützen.</td></tr>
<tr><td>Datenbearbeitung verursacht hohe Risiken</td><td>Durchführung einer DSFA in Form einer «datenschutzrechtlichen Selbstbeurteilung». Können die hohen Risiken trotz zusätzlichen Massnahmen nicht minimiert werden, muss dies dem EDÖB gemeldet werden.</td></tr>
<tr><td colspan="3">Auftragsbearbeitung (Art. 9 nDSG)</td></tr>
<tr><td colspan="2">Der Auftragsbearbeiter bearbeitet Daten nur so, wie es der Verantwortliche tun dürfte (Art. 9 Abs. 1 lit. a nDSG)
Gesetzlich oder vertraglich ist keine Pflicht zur Geheimhaltung vorhanden (Art. 9 Abs. 1 lit. b nDSG)
Der Verantwortliche stellt sicher, dass der Auftragsbearbeiter die Datensicherheit gewährleistet (Art. 9 Abs. 2 nDSG)
Der Auftragsbearbeiter holt vor einer Übertragung des Auftrags an Dritte eine Genehmigung beim Verantwortlichen ein (Art. 9 Abs. 3 nDSG)</td><td>Vor der Auslagerung: Durchführung einer Due Diligence seitens Verantwortlichen und Abgleich mit den internen und rechtlichen Anforderungen (u.a. Datensicherheit, Business-Continuity Management etc.) → Sorgfaltspflicht des Verantwortlichen
Zwischen dem Verantwortlichen und dem Auftragsbearbeiter muss eine Auftragsdatenvereinbarung (ADV) bestehen.</td></tr>
<tr><td colspan="3">Bekanntgabe von Personendaten aus der Schweiz ins Ausland</td></tr>
<tr><td>Drittland mit angemessenem Datenschutz</td><td>Personendaten dürfen ausgelagert werden. (Art. 16 Abs. 1 nDSG)</td><td></td></tr>
<tr><td>Drittland ohne angemessenen Datenschutz</td><td>Bekanntgabe durch Vorhandensein von (Art. 16 Abs. 2 lit a-e nDSG)
Völkerrechtlicher Vertrag
Datenschutzklauseln (vorher dem EDÖB unterbreitet)
Spezifische Garantien
Standarddatenschutzklauseln
Datenschutzvorschriften (unternehmensintern und verbindlich)</td><td>Zu beachten: Die Schrems II-Rechtsprechung hat den Angemessenheitsbeschluss von SCC für Anbieter der USA (oder anderen Drittstaaten ohne angemessenen Datenschutz) für ungültig erklärt. (s. Abb. 12)</td></tr>
<tr><td colspan="2">Zu beachten (Art. 12 nDSG): Die Datenbearbeitung muss in einem Verzeichnis dokumentiert werden.</td><td>Nachweis der datenschutzkonformen Datenbearbeitung.</td></tr>
</table>

Ergänzung zur Bekanntgabe von Personendaten aus der Schweiz ins Ausland:

Unabhängig, ob nun die Daten in ein Land mit oder ohne angemessenen Datenschutz bekannt gegeben werden, ist es essenziell, die Risiken einer Auslagerung zu evaluieren. Dabei geht es um die Analyse technischer und rechtlicher Risiken, welche man als Verantwortlicher verstehen und beurteilen können muss, damit kein unbeabsichtigter Kontrollverlust die Grundrechte und die Privatsphäre der betroffenen Personen verletzen kann. Das Schrems II-Urteil hat im Fall einer grenzüberschreitenden Bekanntgabe in Drittländer ohne angemessenen Datenschutz einigen Wirbel verursacht. Zur Vereinfachung wurde ein kurzer Überblick der Geschehnisse und was in der Zukunft zu erwarten ist, dargestellt.

Abb. 12: Überblick der Rechtsprechungen im Fall einer Übermittlung von Personendaten in ein Land ohne angemessenen Datenschutz



Anmerkung: Eigene Darstellung.

Mittels der SCC wird grundsätzlich bezweckt, eine Lücke in der Gesetzgebung des ausländischen Staats zu füllen, damit die ausgelagerten Personendaten entsprechend den inländischen datenschutzrechtlichen Anforderungen geschützt sind. Die Frage, welche sich nun aber durch die Geschehnisse mit dem Schrems II-Urteil stellt, ist, in welchem

Ausmass die SCC oder andere vertragliche Garantien in den USA durchgesetzt werden können. Die Ausarbeitung des «Trans Atlantic Data Privacy Framework» wird zeigen, inwiefern weitere Garantien für die grenzüberschreitende Datenübermittlung durch den Bundesrat gesprochen oder bestehende ersetzt werden. Auch die Expertinnen und Experten, welche im Rahmen der Forschungsarbeit befragt wurden, gaben zu erkennen, dass durch Abschluss eines Vertrags nicht automatisch die Anforderungen an eine datenschutzkonforme Datenbearbeitung herbeigeführt und die Sicherheit der Daten gewährleistet werden kann.

c) Welchen Beitrag kann der innovative Ansatz von Confidential Computing für den Datenschutz und insbesondere für die Datensicherheit leisten?

Wie in der Antwort zur Frage b) «Datenschutzkonforme Umsetzung einer Datenbearbeitung gemäss nDSG» ersichtlich wurde, müssen für eine Datenbearbeitung die rechtlichen Datenschutzprinzipien eingehalten werden. Für die Einhaltung der Datenschutzgrundsätze werden angemessene TOM eingesetzt. Gleichzeitig ist im Kap. 3 zu «Cloud Computing» beschrieben, dass sich durch die zunehmende digitale Vernetzung, insbesondere die Speicherung und Bearbeitung von personenbezogenen Daten innerhalb einer Cloud, neue rechtliche Anforderungen hinsichtlich der Datenbearbeitung ergeben haben. Aus diesem Grund wird im ersten Schritt der Beitrag von Confidential Computing im Kontext von Cloud-Anbieter beantwortet. Jedoch ist die Technologie generell einsetzbar für den Schutz vor Administratoren Zugriffe[306]

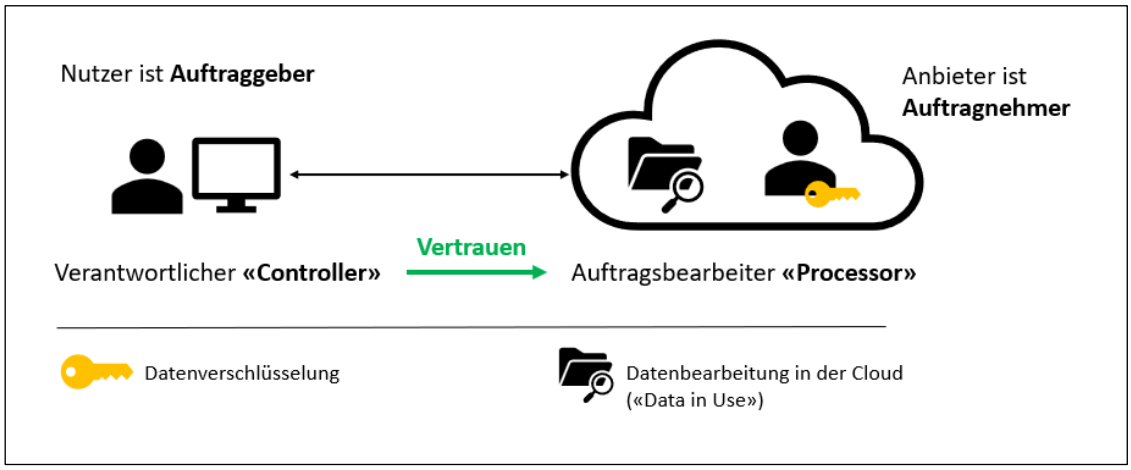
Confidential Computing hat in der Cloud eine hohe Relevanz, da eine Auslagerung von Daten immer einen Kontrollverlust mit sich bringt. Einerseits kann der Serverstandort des Anbieters datenschutzrechtlich hohe Risiken für die Privatsphäre der betroffenen Person auslösen, da der Datenschutz international unterschiedlich ausgelegt wird. Zum anderen ist die Art des genutzten Cloud-Services ausschlaggebend. Werden in einer Cloud lediglich personenbezogene Daten gespeichert («Data at Rest»), können Verantwortliche diese bereits heute durch Verschlüsselung vor Zugriff schützen.

Werden hingegen Daten in einer Cloud bearbeitet («Data in Use»), braucht der Anbieter vollen Zugriff auf die Daten. Diese Zugriffsrisiken können nicht mit jeder Art von personenbezogenen Daten, insbesondere besonders schützenswerte Daten, vereinbart werden.

[306] Vgl. Kap 4.1 «Vertrauen schaffen durch Technik», Abb. 10.

Das Problem rund um die Verschlüsselung und somit der Gewährleistung der Datensicherheit in der Konstellation verschärft sich, wenn ein Cloud-Anbieter die Verschlüsselung kontrolliert und somit Einsicht in die Klartexte hat (s. Abb. 13). Der Auftraggeber muss dem Auftragsbearbeiter (Cloud-Anbieter) vertrauen.

Abb. 13: Auftragsdatenbearbeitung in der Cloud



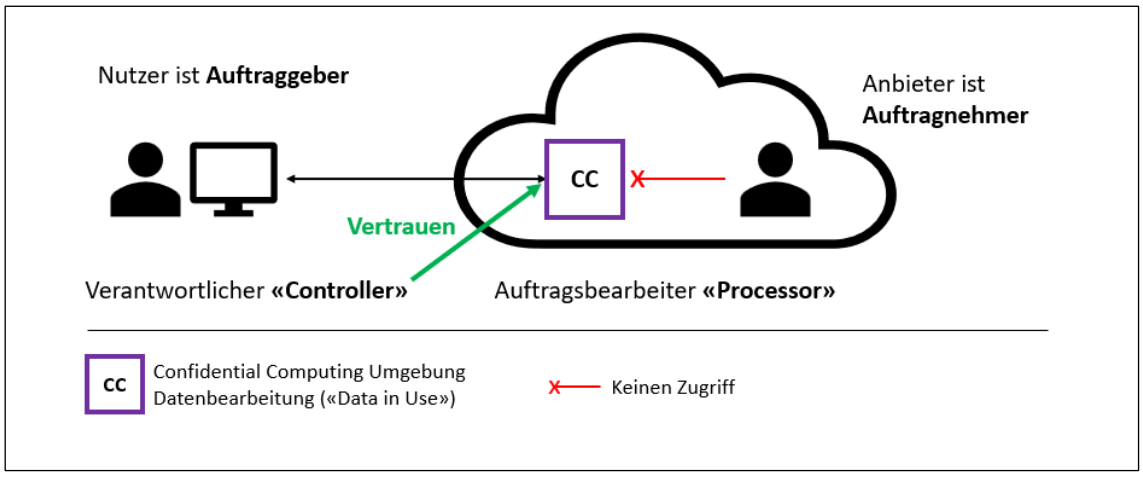
Anmerkung: Eigene erweiterte Darstellung in Anlehnung an JÄGER/RIEKEN/ERNST, S. 9.

Viele Daten werden bereits auf einer Cloud gespeichert. Mittels vertraglicher Bestimmungen zwischen dem Verantwortlichen und dem Auftragsbearbeiter, welche auch das Gesetz fordert, werden die Anforderungen an die Datenbearbeitung definiert, damit die Bearbeitung datenschutzkonform ist und die Datensicherheit gewährleistet werden kann. Die Zusammenarbeit basiert somit grösstenteils auf Vertrauen. Wenn es um die Auslagerung von Daten geht, ist, auch abhängig vom Schutzbedarf der Daten, stets Zurückhaltung seitens der Nutzerinnen und Nutzer vorhanden, vor allem, wenn besonders schützenswerte Daten gemäss Art. 6 lit c nDSG bearbeitet werden. In diesem Bereich bestehen u.a. viele Datensicherheits-Bedenken bzgl. des Zugriffs des Anbieters.

Confidential Computing bietet als innovative Technologie in dieser Hinsicht eine Lösung für die Vertraulichkeit einer Datenbearbeitung, welche gewisse Sicherheitsrisiken eliminiert. Confidential Computing führt eine isolierte Enklave ein, welche die Möglichkeit bietet, risikoreiche Datenbearbeitungen durchzuführen, welche bisher nicht datenschutzkonform ausgeführt werden konnten. Der Schutz der Daten wird zu jederzeit gewährleistet und der Zweck der Datenbearbeitung wird im Voraus technisch definiert.

Die Gewährleistung von Datensicherheit wird gemäss nDSG[307] durch das Treffen von geeigneten technischen Massnahmen erreicht. Mit Confidential Computing wird anhand einer technischen Lösung der Zugriff auf die Daten verhindert und die Datensicherheitsrisiken minimiert. Eine organisatorische Massnahme, welche Vertrauen zwischen dem Anbieter und dem Verantwortlichen schafft, wird somit durch eine technische Massnahme ersetzt. In der Folge bedeutet das, dass weder die Administratoren der Cloud noch die Softwareentwickler Zugriff auf die Daten haben. Das Vertrauen basiert somit auf der Technik. Technische Eigenschaften wie die «Remote Attestation» ermöglicht die Prüfung der Integrität einer Confidential Computing-Umgebung. «Encryption in Use» stellt sicher, dass die Daten während der Bearbeitung vor Zugriff geschützt sind.

Abb. 14: Datenbearbeitung in einer Confidential Computing-Umgebung



Anmerkung: Eigene erweiterte Darstellung in Anlehnung an JÄGER/RIEKEN/ERNST, S. 9.

Gemäss Aussagen der Experten dürfte, basierend auf den Anforderungen an technische Massnahmen und im Kontext der Schrems II-Rechtsprechung, im Fall einer Datenanalyse, welche in einer Confidential Computing-Umgebung durchgeführt wird, das Kriterium des Serverstandorts keinen Einfluss mehr haben. Juristische Beurteilungen zu dieser Ausganglage sind jedoch noch ausstehend.

Betrachtet man zudem den Fall einer geplanten Datenbearbeitung von Personendaten in einem Land ohne angemessenen Datenschutz (vgl. Frage b) und dass nach der Durchführung eines TIA hohe Restrisiken verbleiben, kann Confidential Computing als technische Lösung eingesetzt werden, um gewisse Datenbearbeitungen datenschutzkonform umzusetzen. Hohe Restrisiken können auch nach der Durchführung einer DSFA bestehen.

[307] Art. 8 nDSG

Confidential Computing kann, abhängig von der Art der Datenbearbeitung, auch für jene Restrisiken eine Möglichkeit für die datenschutzkonforme Umsetzung der Datenbearbeitung bieten.
Ein Unternehmen schützt sich mit Confidential Computing sowohl gegen unberechtigten Zugriff in der Cloud als auch beim Einsatz auf internen Server gegen unerlaubten Zugriff durch Interne.
Die folgenden Anwendungsbeispiele zeigen Datenbearbeitungen auf, welche durch herkömmliche technische und organisatorische Massnahmen in punkto Datensicherheit hohe Risiken aufweisen, jedoch durch die Nutzung von Confidential Computing datenschutzkonform ausgestaltet werden können.

Gesundheits- und Pharmabranche:
Die besonders schützenswerten Daten, welche Gesundheitsinstitutionen für eine Kollaboration zur Verfügung stellen, sind durch Confidential Computing, resp. während der Bearbeitung innerhalb dieser «Data Clean Rooms» geschützt und bleiben in der Kontrolle der Gesundheitsinstitution.[308] Bereits heute wird für die Prüfung von Forschungsmodellen aus der Pharmabranche Confidential Computing angewendet.

Marketing:
Durch die baldige Abschaffung der «Third Party Cookies»[309] sind Unternehmen gezwungen, einen anderen Weg für personalisierte Werbung zu schaffen und gleichzeitig die Datenschutzprinzipien einzuhalten. Die Daten der Kundinnen und Kunden müssen weiterhin geschützt und deren Privatsphäre gewahrt werden. Mit Confidential Computing lassen sich «First Party Data» eines Unternehmens mit den «First Party Data» eines Drittunternehmens analysieren, ohne, dass die Unternehmen Zugriff in die jeweils fremden Daten haben. Die gewonnenen Erkenntnisse können dann für das effiziente Platzieren von Werbung genutzt werden.

Sekundärnutzung von besonders schützenswerten Daten:
Die rechtliche Ausgestaltung im Bereich der besonders schützenswerten Daten insbesondere Gesundheitsdaten ist sehr komplex. Gesundheitsdaten werden im nDSG zudem nicht

[308] Mehr Informationen unter https://blog.decentriq.com/decentriq-roche-partnership-featured-on-microsofts-azure-confidential-computing-webinar-series/ ; https://blog.decentriq.com/data-collaboration-made-simple-and-safe-applications-in-the-health-care-sector/
[309] Vgl. Kap. 8.4.1

explizit definiert, weshalb der jeweilige Kontext, in dem die Gesundheitsdaten generiert werden, analysiert werden muss. Da Gesundheitsdaten aufgrund ihrer Beschaffung (genetische, biometrische Daten) tendenziell eine einfachere Re-Identifikation ermöglichen, bestehen hohe Anforderungen an deren Anonymisierung. Confidential Computing könnte diesen Sachverhalt anhand der technischen Verschlüsselung lösen, was bereits in einem Gutachten[310] erwähnt wurde. Sollten besonders schützenswerten Daten vollständig anonymisiert verfügbar gemacht werden können, würden diese nicht mehr unter den Geltungsbereich des nDSG fallen, worauf auch der bestimmte Zweck, welcher für die datenschutzkonforme Datenbeschaffung notwendig ist, entfallen würde. Die Herausforderung besteht in der Erweiterung des Zwecks. Durch die Inkraftsetzung eines gesetzlichen Rahmens könnte in diesem Sachverhalt zusätzlich mehr Klarheit geschafft werden. Die zukünftigen Entwicklungen im Parlament werden es zeigen. In diesem Kontext gilt es jedoch auch gesetzliche Grundlagen, welche Vorrang haben, sogenannte «lex specialis» zu berücksichtigen. Das Humanforschungsgesetz spielt im vorliegenden Kontext eine entscheidende Rolle.

Abschliessend konnte aufgrund der Ergebnisse aus den Experteninterviews festgestellt werden, dass Rahmenwerke und vertragliche Garantien zwischen Verantwortlichen und Auftraggeber, welche eine datenschutzkonforme Datenbearbeitung sicherstellen sollen, nicht gewährleisten, dass die Datenbearbeitungen auch tatsächlich datenschutzkonform ausgeführt werden und die Datensicherheit gewährleistet wird. Es wurde betont, dass rein organisatorische Massnahmen für die Einhaltung nicht mehr ausreichen und man eine technische Lösung einsetzen muss. Im Allgemeinen wird jedoch die Ausgestaltung einer technischen Lösung, welche einen vollumfänglichen Schutz bietet, aufgrund potenzieller Schwachstellen, nie umsetzbar sein. Jedoch leistet der Einsatz von Confidential Computing als technische Massnahme einen wesentlichen Beitrag zu einer sichereren und datenschutzkonformen Datenbearbeitung.

[310] Mehr Informationen unter https://www.interpharma.ch/wp-content/uploads/2022/10/Gutachten-Interpharma_Sekundaernutzung-Gesundheitsdaten.pdf

10 Kritik

Die Thematik der Forschung bedingte mit der fachlichen Auseinandersetzung von Technologie und Recht zwei Themenschwerpunkte. Vor allem im technischen Bereich war es eine Herausforderung, eine geeignete Flughöhe zu finden, welche in Zusammenhang mit den rechtlichen Anforderungen ein nachvollziehbares Verständnis ermöglicht. Die Tatsache, dass in der Literatur die Nutzung von technischen Begrifflichkeiten teilweise unterschiedlich gehandhabt wird, zeigte zusätzlich auf, dass für das Gesamtverständnis der Thematik eine vertiefte Einarbeitung vorausgesetzt wird. Dies hat sich positiv auf die Durchführung der Experteninterviews ausgewirkt. Die Expertinnen und Experten waren in ihren jeweiligen Bereichen sehr fundiert, was der Forschung viele wertvolle Erkenntnisse einbrachte. Dennoch war es eine Herausforderung, eine spezifische Technologie wie Confidential Computing in einen gesetzlichen Kontext zu setzen, da es noch an Erfahrung und an Best-Practice-Beispielen fehlt.

Der Einbezug von Trusted Computing mittels fundierter Recherche ermöglichte das Nachvollziehen der technischen Entwicklung von einem vertrauenswürdigen Betriebssystem hin zu Confidential Computing. Der Einbezug von Cloud Computing ebnete den Weg, um eine Brücke zwischen den ersteren zwei Technologien zu schlagen. Dieser Ansatz wird deswegen nach wie vor als sinnvoll erachtet.

Die Interpretation des nDSG war zum Zeitpunkt der Forschung teilweise erschwert, da sich viele Einschätzungen seitens des EDÖB auf das bestehende Datenschutzgesetz bezogen. Bis zur Inkraftsetzung am 1. September 2023 dürften noch einige Aktualisierungen stattfinden.

Zu guter Letzt ist in der vorliegenden Forschung zu berücksichtigen, dass eine Momentaufnahme der technischen Gegebenheiten und der vorherrschenden rechtlichen Normen aufgezeigt wird. Einerseits scheint das grundlegende technische Wissen über Confidential Computing zu existieren, aber die Nutzung von Confidential Computing für die datenschutzkonforme Datenbearbeitung steckt in der Schweiz noch in der Anfangsphase. In der Ausarbeitung von gesetzlichen Rahmenwerken findet zudem vor allem auf internationaler Ebene momentan viel Bewegung statt, worauf eine Einschätzung des EDÖB zu gegebener Zeit zu erwarten ist.

11 Ausblick

Der Fortschritt der Technologien im Bereich der Digitalisierung schreitet rasant voran. Die Herausforderung besteht nun aus regulatorischer Sicht, mit diesem Fortschritt mitzuhalten und Bestimmungen zu erlassen, welche praktikabel sind und aufzeigen, welche Datenbearbeitungen in welchem Rahmen möglich sind. Best-Practice-Beispiele könnten für die Nutzung von Confidential Computing wegweisend sein. Die Zukunft wird zeigen, inwiefern durch technische Massnahmen, wie das bei Confidential Computing der Fall ist, risikoreiche Datenbearbeitungen durchgeführt werden. Fakt ist, dass die Anforderungen an den Schutz der Privatsphäre von Personendaten nicht abnehmen, sondern in der Tendenz zunehmen werden. Weitere technische Möglichkeiten wie die «Homomorphic Encryption» stehen bereits in den Startlöchern. Es stellt sich die Frage, wie viel Vertrauen man in die Technologien hat und wie viele Best-Practice-Beispiele und Richtlinien notwendig sind, das Vertrauen aufzubauen.

Anhang

Wahrheitserklärung

Ich bestätige mit meiner Unterschrift, dass ich die vorliegende Arbeit selbständig und ohne Mithilfe Dritter verfasst habe und in der Arbeit alle verwendeten Quellen angegeben habe.

Gleichzeitig nehme ich zur Kenntnis, dass die ausschliesslichen Verwendungsbefugnisse dieser Arbeit bei der ZHAW School of Management and Law liegen. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Lenzburg, 30. Mai 2023

_____

Adrienne Remund

Leitfaden Experteninterview

Einschätzung aus dem beruflichen Alltag (Häufige Fragestellungen, Trends der Branche, Nachfrage der Kunden)

1. Welche Bedürfnisse haben die Kunden momentan, wenn es um den Schutz von personenbezogenen Daten und Datenbearbeitung geht?
2. Was ist ein Treiber von Kunden, Confidential Computing einzusetzen? (rechtlich, technisch)?

Technischer Bereich

1. Wie verändert Confidential Computing die Datenbearbeitung? Was ist der Mehrwert?
2. Kann der Zugriff auf die Daten vollständig ausgeschlossen werden? (Zugriff von Anbieter, Zugriff von Herstellerfirmen, Chip, Cloud-Anbieter etc.)

Gesetzlicher Bereich

1. Cloud Computing: Was sind die gesetzlichen Risiken? Art der Daten, Territorial?
2. Wie verändert CC die Datenschutzkonformität von besonders schützenswerten Personendaten?
3. Wie kann der Kunde die Integrität von Confidential Computing prüfen und im Sinne der Datenschutzkonformität beweisen?

Transkript 1

Experteninterview mit Christoph Ernst, Cloud Solution Architect, Microsoft Switzerland

Frage: Betrachten wir den Wandel von Cloud Computing und machen eine kleine Marktanalyse. Inwiefern hat sich die Nachfrage nach Cloud Infrastrukturen verändert und wie haben sich die Bedürfnisse der Kunden dabei verändert?

[1] Antwort: Was ich festgestellt habe, ist, dass der Wandel von «man hat alles in seinen eigenen vier Wänden» versus der Cloud, wo man nicht ganz genau weiss, wo die Server sind, Tatsache ist. Firmen migrieren in die Cloud, das lässt sich nicht mehr aufhalten. Die Vorteile der Cloud wie die Agilität sowie auch der schnelle Innovationszyklus werden wahrgenommen.

Es stellt sich dann die Frage: Wie schütze ich Personendaten, gemäss der aktuelle Gesetzgebung, wenn die Daten nicht mehr auf «meinem» Server liegen. Dabei ist der Vertrauensaufbau sehr wichtig. Microsoft lässt die ganze Infrastruktur anhand externer Gutachten überprüfen. Kunden können unter servicetrust.microsoft.com auf eine Vielzahl von Reports zu Data Privacy und Data Protection zugreifen. Microsoft investiert viel dafür, dass die Cloud Infrastruktur, welche den Kunden zur Verfügung gestellt wird, gemäss den heute geltenden Regulierungen betrieben wird.

[2] Die Cloud Infrastruktur funktioniert nach dem Shared Responsability Modell[311]. Shared Responsability zeigt auf, welche Sicherheitsaufgaben vom Cloudanbieter und welche Aufgaben vom Kunden verantwortet werden. Am Beispiel des on-prem Model sehen wir, dass der Kunde für sämtliche Sicherheitsaufgaben verantwortlich ist. Für die physische Sicherheit des DataCenters, die Zugangskontrollen, die Stromzufuhr, das Netzwerk, die Server, das Operating System (Windows, Linux) die Applikationen und Daten. In der Cloud verschieben sich die Verantwortlichkeiten. Bei Infrastructure as a Service (IaaS) können Kunden virtuelle Server provisionieren. Microsoft zeigt sich verantwortlich für das Netzwerk, das Datacenter und den Virtualisierungslayer. Der Rest verbleibt in der Verantwortung des Kunden. Je veredelter der Service (PaaS, SaaS), desto mehr übernimmt Microsoft. Wichtig zu verstehen ist, dass die Hoheit der Daten immer beim Kunden bleiben. Zusammen gefasst bedeutet das: Der Provider ist verantwortlich für die Sicherheit der Cloud (Security of the Cloud), während dem der Kunde

[311] https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

die Verantwortung für die provisionierten Services in der Cloud hat (Security in the Cloud).

Frage: Was schützt Confidential Computing (CC) und was ist neu an dieser Technologie?

[3] Antwort: Confidential Computing schützt Daten, die gerade von einem Computer System verarbeitet werden (Data in Use) vor unberechtigten Zugriffen. CC wird am Markt wahrgenommen ist aber noch nicht stark verbreitet. Mittels Confidential Computing Samples[312] Kunden können CC-Testapplikationen nutzen. Häufig stellt sich heraus, dass die Komplexität einer Confidential Computing Applikation unterschätzt wird. In den USA gibt ein Use Case in der Health Industrie, in welchem CC produktiv zum Einsatz kommt[313]. Verschiedene Gesundheitseinrichtungen steuern private Gesundheitsdatasets bei, um ein Machine Learning-Modell zu trainieren. Die einzelnen Einrichtungen haben jeweils nur Zugriff auf ihr eigenes Dataset. Die Daten und das Trainingsmodell sind weder für eine andere Einrichtung noch für den Cloudanbieter sichtbar.

Frage: Wenn du jetzt eine Infrastruktur bauen müsstest, welche technische Anforderungen müssen gestellt werden, damit der Schutz von besonders schützenswerten Daten gewährleistet ist?

[4] Antwort: Ich würde mit einem Provider zusammen arbeiten wollen, der Regulierungen und Standards erfüllen und aktuell halten kann. Die zugrundeliegende Infrastruktur muss fähig sein mit besonders schützenswerten Daten umzugehen und diese Fähigkeit muss regelmässig überprüft werden. Ebenso gilt es, die Infrastruktur, welche der Kunde in der Cloud aufbaut, mit Security Best Practices zu schützen. Least Privilege, Logging und Monitoring, Schutz des Endpoints und die Ausbildung der User in Security und Compliance relevant. Die Verschlüsselung geniesst, bei besonders schützenswerten Daten, besonders viel Aufmerksamkeit. Fragen wie: «Wo liegt das Schlüsselmaterial? Wie ist dieses gesichert? Und wer darf das Schlüsselmaterial verwenden?» müssen geklärt sein und im Einklang mit den Vorgaben stehen.

[312] https://github.com/Azure-Samples/confidential-computing
[313] https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios#secure-multi-party-computation

Frage: Schlussendlich fragt man sich ja auch vor allem bei besonders schützenswerten Daten, wie der Schlüssel gespeichert wird, damit nur ich Zugriff habe. Funktioniert das überhaupt?

[5] Antwort: Das Schlüsselmaterial liegt bei besonders schützenswerten Daten vorzugsweise in einem Hardware Security Modul (HSM) vom Cloud Provider oder vom Kunden. Die HSMs stellen sicher, dass das Schlüsselmaterial geschützt ist und nicht exportiert werden kann. Aber das ist nur die halbe Miete, denn wenn mit den Daten gearbeitet wird, liegen sie, zu diesem Zeitpunkt, in unverschlüsselten Zustand vor. Es wäre also möglich beispielsweise den Arbeitsspeicher auszulesen und somit Zugriff auf die Daten zu erlangen. Um diesem Vorgehen vorzubeugen, gibt es die eingangs erwähnten Zertifizierungen. Die Administratoren der Cloud-Infrastruktur haben grundsätzlich keinen privilegierten Zugang zum Hypervisor (Standing Access). Dieser muss immer wieder beantragt werden, zum Beispiel, wenn ein Support Case vorliegt.

Frage: Was macht nun CC für einen Unterschied?

[6] Antwort: Wie eben beschrieben besteht im Fall von Data in Use ein gewisses Risiko. Gespeicherte (Data at Rest) und fliessende Daten (Data in Transit) können ohne Problem verschlüsselt und gesichert werden, was bei den Daten, welche gerade berechnet werden (Data in Use), nur bedingt der Fall ist. CC schliesst diese Lücke.
Confidential Computing erstellt eine hardwarebasierte, vertrauenswürdige Ausführungsumgebung (Trusted Execution Environment, TEE). Die TEE ist also eine Umgebung, mit der die ausschliessliche Ausführung von autorisiertem Code erzwungen wird. Für alle Daten in der TEE ist es nicht möglich, dass sie mit Code, der sich ausserhalb dieser Umgebung befindet, gelesen oder manipuliert werden.
Aber wie Eingangs dieses Interviews erwähnt, arbeite ich noch mit keinem Kunden zusammen, der dies produktiv im Einsatz hat.

Frage: Das bedeutet, das Interesse an CC ist noch nicht so gross?

[7] Antwort: Richtig - noch nicht. Es wird komplex und auch kostspielig, wenn man eine Applikation mit CC schützen möchte. Auch ist das Wissen darüber noch nicht stark verbreitet. Entwickler, die Confidential Computing verstehen und richtig umsetzen können, sind schwierig zu finden.
Auch gilt es abzuwägen, ob Confidential Computing tatsächlich nötig ist, um den Schutzbedarf der Daten zu erfüllen. Ich mache die Erfahrung, dass dies oft erfüllt

werden kann, wenn eine Cloud Infrastruktur sorgfältig aufgebaut wird. Security Best Practices, Verschlüsselung und dem Schutz der Schlüssel kommt dabei eine zentrale Bedeutung zu. Auch können zwei Schlüssel[314] zum Einsatz kommen. Ein Schlüssel, den der Cloud Provider gar nie sehen kann. Dies schränkt aber die Funktionalität der Cloud ein.
Der Schlüssel soll in jedem Fall in einem HSM und unter der vollständigen Kontrolle des Kunden stehen. Das HSM erfüllt die notwendigen Zertifizierungen, um die Sicherheit der Schlüssel zu garantieren.
Noch nicht gesprochen haben wir über Data-Residency. Im Fall von besonders schützenswerten Daten, ist es wichtig, dass sichergestellt werden kann, dass die Daten in der Schweiz, oder einer anderen vom Kunden gewünschte Region, verbleiben. Microsoft hat in der Schweiz zwei so genannte Regions (Switzerland North und Switzerland West) bestehend aus mehreren Data Centern. Die Kunden verwalten eigenständig, wo die Daten gespeichert und bearbeitet werden.
Damit ist meiner Meinung nach ein grosser Teil der nötigen Schutzmassnahmen getroffen. Oder fehlt noch was?

Frage: Die Daten in Bearbeitung?
[8] Antwort: Das kann mit den Reports und den Compliance Standards beantwortet werden. Wenn verglichen wird, was Cloud Umgebungen alles unternehmen, um Kundendaten zu schützen und was eine on-prem Umgebung dafür tun kann, denke ich stehen Clouds in nichts nach.

Frage: Bezieht sich deine Aussage auf personenbezogene sowie besonders schützenswerte Daten?
[9] Antwort: Kunden mit besonders schützenswerten Daten sind noch zurückhaltend gegenüber der Cloud. Obwohl es Beispiele von erfolgreichen Projekten gibt. Kann sein, dass das Risiko der Early-Mover noch etwas gross eingeschätzt wird.

Frage: Hat das neue Datenschutzgesetz eine Welle von Kundenanfragen ausgelöst?
[10] Antwort: Bei mir persönlich nicht. Liegt womöglich daran, dass ich erst ins Spiel komme, wenn alle rechtlichen Anforderungen geklärt sind und die Architektur-Phase

[314] https://learn.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide

beginnt. Ich vermute, dass andere Rollen mehr vom neuen Datenschutzgesetz betroffen waren.

Frage: Sie haben die Server in der Schweiz erwähnt. Gibt es bzgl. der Datenübermittlung ins Ausland Bedenken der Kunden?

[11] Antwort: Wir garantieren den Kunden den Datenstandort. Es wurde eigens eine sogenannte EU Data-Boundary[315] eingerichtet. Die Data-Boundary ist eine geografisch definierte Grenze, innerhalb derer Microsoft sich verpflichtet hat, Kundendaten zu speichern und zu verarbeiten. Die EU Data-Boundary umfasst die Länder der EU einschliesslich der Schweiz. Offenbar konnten damit Bedenken von Kunden aufgefangen werden.

Ich betone gerne, dass Microsoft einiges unternimmt, um die Daten der Kunden zu schützen und geschützt zu halten. Der Microsoft Law Enforcement Requests Report[316] beispielsweise gewährt Einblick wie häufig Microsoft von Behörden angefragt wurde Kundendaten auszuhändigen

Frage: Machen wir einen Blick in die Zukunft. Wo sehen Sie die Trends und zukünftigen Herausforderungen in der Datenbearbeitung?

[12] Antwort: Spontan kommt mir Big Data in den Sinn. Für Provider und Kunden ist und wird dieser Bereich sehr spannend. Es geht darum, alle möglichen Daten und Signale in einem grossen Topf zu werfen und daraus Schlüsse zu ziehen. So werden, unter anderen, Signale zum Nutzen der Security ausgewertet. Da sprechen wir von Metadaten, was zum Beispiel Login-Daten oder IP-Adressen beinhaltet. Es gibt so viele Events auf Infrastrukturen wie M365 oder der Gaming Infrastruktur. Können Abweichungen von der Norm ausgemacht werden? Gibt es auffällige Muster? Gleichzeitig stelle diese Big Data Pools meiner Meinung nach auch ein Risiko dar. Können in Zukunft Schlüsse aus solchen Pools gezogen werden, welche heute nicht beabsichtigt sind? Das wird uns in Zukunft sicherlich beschäftigen.

Ende des Experteninterviews.

[315] https://learn.microsoft.com/de-de/privacy/eudb/eu-data-boundary-learn
[316] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Transkript 2

Experteninterview mit David Sturzenegger, Produkteverantwortlicher Decentriq

Frage: Was ist der Hauptreiber für Kunden, Confidential Computing einzusetzen?

[1] Antwort: Das ist eine gute Frage. Meistens geht es um die Confidentiality. Es gibt viele unterschiedliche Anwendungsbereiche bei Confidenital Computing (CC). Wir bei Decentriq konzentrieren uns auf Datenkollaborationen. Das bedeutet, dass mehrere Parteien Daten zusammenbringen und analysieren, ohne dass man die Daten den anderen Parteien Preis geben muss. Ohne Confidential Computing oder andere ähnliche Technologien muss die eine Partei typischerweise der anderen Partei die Daten freigeben oder umgekehrt, oder einer Drittpartei. Auf einem Weg jedenfalls müssen die Daten preisgegeben werden. Oft will oder kann man das nicht. Da sind wir beim Thema Datenschutz. Das ist der Bereich, auf den wir uns primär fokussieren. Wir haben eine Software as a Service-Plattform gebaut, welche komplett in CC betrieben wird. Dort haben wir sogenannte Datenräume, welche man nach Bedarf konfigurieren kann. Möchten zwei Parteien zusammenarbeiten, wird vereinbart, welche Partei welche Art von Daten einbringt. Das wird in den Datenraum geschrieben und es werden Berechnungen ausgeführt mittels Python, SQL etc. Die eine Partei erhält dann ein Resultat und die andere erhält ein Audit-Log, in welchem ersichtlich ist, was gemacht wurde. Das wäre eine mögliche Konfiguration eines solchen Datenraums. Da dies alles mit CC läuft, kann auf die Daten der beiden Parteien weder zugegriffen noch die Definition des Datenraums verändert werden. Das ist unser Kernprodukt. Dann gibt es andere CC-Vendors mit anderen Use Cases, wie das eine Security Feature «Encryption in Use», welches CC ermöglicht, da es noch ein bisschen sicherere ist. Es ist tatsächlich nicht so schwierig, diesen Aspekt von CC zu nutzen.

Frage: Ist es eher ein rechtlicher Treiber oder technischer Treiber, der die Kunden, dazu bringt, CC zu nutzen? Kommen die Kunden zu euch oder müsst ihr aktiv auf die Kunden zugehen?

[2] Antwort: Es ist immer so, dass man, wenn man etwas Neues baut, zuerst sehr viel outbound betreiben muss und sich dann inbound daraus entwickelt. Ich würde aber behaupten, dass wir momentan eher noch auf die Kunden zugehen müssen. Es nähert sich an. Betrachtet man die unterschiedlichen Kundensegmente und Branchen, fokussieren wir uns hauptsächlich einerseits aufs Marketing, genauer gesagt digitales Marketing, wo

es um die Fragestellung geht, wie man Daten nutzen kann, ohne die Privatsphäre der Kundinnen und Kunden zu verletzen. Andererseits haben wir einen Fokus im Gesundheitsdatenbereich, wo es darum geht, wie man die Gesundheitsdaten nutzen und den Datenschutz auf einem hohen Niveau erhalten kann. Dabei geht es auch um die Sekundärnutzung von Gesundheitsdaten. Dann haben wir noch ein paar andere Projekte mit Banken und Versicherungen, welche für Kundenanalysen die Daten vergleichen möchten. Grundsätzlich ist das Konzept immer gleich. Es gehen personenbezogenen Daten herein und es kommen aggregierte, anonymisierte Daten heraus. Das ist der gemeinsame Nenner. Im Bereich der Gesundheitsdaten führen wir eine Zusammenarbeit mit der Roche. Dabei hat Roche ein Modell, welches sie in einem Spital validieren lassen möchten. Das Spital besitzt Daten zu einer bestimmten Krankheit, welche in dieses Modell eingespeist werden können. So kann gemessen werden, wie geeignet das Modell ist, um vorherzusagen, dass eine Person krank ist. Das ist ein Modell, welches für die Roche sensitiv ist. Zudem werden Gesundheitsdaten eines Spitals genutzt, welche auch sensitiv sind. In einem solchen Case kann die Plattform von Decentriq genutzt werden und das Resultat anhand eines Reports gezogen werden. Wir sind momentan eher involviert im Online-Marketing-Bereich, wo das Thema der «Data Clean Rooms» ein grosses Thema ist. Es gibt sehr viele unterschiedliche Anbieter von «Data Clean Rooms». Dieser Megatrend folgt der Tatsache, dass diese Third Party Cookies bald komplett gestrichen werden. Sobald bspw. der Chrome Browser das auch als Default Option drin hat, gibt es keine Möglichkeit mehr, Nutzer über mehrere Websites zu tracken. Diese Tatsache eliminiert jedoch das halbe Advertising-Ökosystem. Deswegen gibt es einen Trend, Daten zu nutzen, welche sog. First Party Data sind. Bspw. Nike weiss, wer welche Schuhe bei ihnen im Online Store kauft. Jetzt möchten sie bspw. über eine Onlinezeitung ähnliche Leute ansprechen. Ich möchte und darf meine Kundendaten nicht dem Zeitungsverlag senden, sondern kann diese dann in einem Datenraum schleusen und ähnliche Personen finden, welche über die Zeitung angesprochen werden können, ohne dass jemand ausserhalb Einsicht in die Daten erhält. Es ist öffentlich, dass wir mit Goldbach zusammenarbeiten, welche bspw. Tamedia vermarktet. Dort gibt es sehr viele Use Cases momentan. Es geht immer darum, wie wir die sensitiven Personendaten besser schützen können und was aus rechtlicher Sicht ermöglicht wird.

Frage: In Zusammenhang mit dem rechtlichen Aspekt stellt sich nun die Frage, ob die Nutzung von CC in der EU datenschutzkonform ist auch für schützenswerte Daten?

[3] Antwort: Im Kontext der Datenschutzkonformität stellt sich immer die Frage, welchen Use Case wir betrachten. Aus CC ergibt sich nicht automatisch Datenschutzkonformität. Was jedoch klar ist, dass CC sicherer ist. Jetzt stellt sich die Frage der Güterabwägung, wie bspw. zwischen Legitimate Interest und Impact of Data Subject. Wenn es um die Nutzung der Daten geht, besteht auf der Seite des Impacts das durch die Datenbearbeitung entstehenden Risiko. Das wird durch CC fast auf null minimiert. Man hat eine Box, aus der nur anonyme Daten generiert werden, verglichen zur anderen Option, bei der man die Liste an Goldbach sendet auf der Basis eines Versprechens ihrerseits, dass die Daten durch sie nicht eingesehen werden. Da besteht mit CC ein grosser Vorteil und wir haben gewisse rechtliche Meinungen, welche Aussagen, dass man das Gewicht eher auf den Legitimate Interest setzt. Im Gesundheitsbereich haben wir diesbezüglich jedoch noch keine klare Meinung.

Frage: Ist der Zugriff auf Personendaten, welche mit CC bearbeitet werden, wirklich durch gar niemanden möglich? Intel ist ja auch im Loop vorhanden, da sie die Chips liefern.

[4] Antwort: Wie immer gibt es nie 100% Sicherheit. Intel ist bei dieser Technologie im Loop of Trust und könnte theoretisch mit uns zusammenarbeiten um an sensitive Daten zu kommen. Technologien können im Allgemeinen auch Schwachstellen aufweisen, welche man noch nicht entdeckt hat. Es geht jedoch immer darum, eine Risikoabwägung zu erstellen. Auch wenn es bspw. darum geht, dass Daten in die USA fliessen. Für alle Praxisgründe haben wir CC als sehr sicher eingestuft.

Frage: Sehen das die Kunden gleich? Gibt es grosse Bedenken auch im Kontext der USA?

[5] Antwort: Vor drei Jahren gab es tatsächlich solche Diskussionen. Davon haben wir mittlerweile keine mehr.

Frage: Was hat sich in der Zwischenzeit geändert?

[6] Antwort: Es gibt generell einen Trend für die Cloud in gewissen Hinsichten und CC ist in diesem Kontext noch sicherer. Daraus resultieren noch weniger Bedenken. In

vielen Use Cases wird die Cloud generell als sicherer eingestuft, da sich viele Firmen keine eigene Security Abteilung leisten können. Wenn man jetzt mit CC beweisen kann, dass Microsoft nicht auf die Daten zugreifen kann, dann sind die Kunden zufriedengestellt. Wir kämpfen eher damit, dass vor allem im Medienbereich der Nutzen hinterfragt wird, resp. es kommt die Frage auf, ob die Daten wirklich in diesem Ausmass geschützt werden müssen.

Frage: Wie kann denn kundenseitig die Integrität von CC geprüft werden?

[7] Antwort: Super Frage. Im Prinzip stellt CC zwei Security Properties sicher, welche man sonst nicht hat. Das eine ist die Verschlüsselung der Daten im Arbeitsspeicher, die sog. Encryption in Use. Das hilft, dass andere Programme nicht auf den Arbeitsspeicher zugreifen können oder der Arbeitsspeicher vom Computer heruntergeladen und irgendwo anders wieder hochgeladen und gelesen werden könnte. Das zweite ist Remote Attestation. Das bedeutet, dass der Endnutzer unabhängig und eindeutig verifizieren kann, dass die Decentriq Plattform in CC läuft. Da geht es um Verschlüsselungen, welche in der CPU sind, etc. Wenn es das nicht gäbe, müsste man immer noch dem Anbieter einfach vertrauen, dass die Daten mit CC bearbeitet werden. Unter der Remote Attestation kann verifiziert werden, dass die Daten mit CC bearbeitet werden und anhand welcher Codes die Berechnungen laufen.

Frage: Für welche Art von Daten ist CC ein USP?

[8] Antwort: Es ist sehr einfach in der Nutzung, deswegen ist es grundsätzlich für alle sensitiven Daten, welche von einer Firma herausgegeben werden, anwendbar. Viele Use Cases wie Datenkollaborationen oder Spitäler, welche im Rahmen einer Forschung Daten in einem geschützten Umfeld zur Verfügung stellen, empfehle ich die Nutzung von CC. Für Use Cases, bei denen die andere Partei direkte Einsicht in die Daten benötigt, dort macht es keinen Sinn.

Frage: Welche Restrisiken gibt es bei CC?

[9] Antwort: Intel ist das eine, Unkowns in der Technologie sind das andere. Das grösste Restrisiko ist womöglich falsches Nutzerverhalten. Menschliches Versagen ist bei jeder Technologie ein Thema.

Frage: Lässt sich das menschliche Versagen minimieren?

[10] Antwort: Ja, wir haben die Software bereits so gebaut, dass nach einer Analyse mit CC nur anonyme Daten herausgegeben werden. Man nennt dies Output Privacy. Bspw. werden keine kleinen Datensätze (<50) herausgegeben.

Frage: Zum Schluss machen wir einen Blick in die Zukunft. Was sind die Trends und Herausforderungen in der Datenbearbeitung?

[11] Antwort: Ich glaube, das grosse Problem stellt sich in der Vereinbarung des Mehrwerts der Datennutzung mit dem Datenschutz. Die EU hat mit dem GDPR die Möglichkeiten bereits sehr eingeschränkt und das ist grösstenteils gut so. Andere Rechtsprechungen sehen das ein bisschen lockerer. Mit CC oder auch anderen Technologien wie Homomorphic Encryption kann man Utility und Privacy gleichzeitig erreichen. Das ist sicherlich ein Teil der Lösung. Im Bereich der Datenbearbeitung besteht sicherlich die Frage, wie man bei einer Sekundärnutzung von Daten den daraus entstehenden Mehrwert sicherstellen kann und dabei gleichzeitig die Privatsphäre und den Datenschutz gewährleistet. Wie lässt sich eine intelligente Regulierung erstellen, welche Personendaten schützt aber nicht alles andere ausbremst. Es gibt so viele Gesetze in der Schweiz, dass es oft schwierig ist, im gegebenen Kontext herauszufinden, was nun erlaubt ist und was nicht. Diese Gratwanderung stellt für uns eine wesentliche zukünftige Herausforderung dar.

Ende des Experteninterviews.

Transkript 3

Experteninterview mit Matthias Eigenmann, Legal Counsel – Technology and Privacy

Frage: Was ist kritisch bei der Auslagerung der Personendaten auf eine Cloud auch hinsichtlich von Confidential Computing (CC)?

[1] Antwort: Vorab muss man verstehen, dass CC nicht zwingend eine Cloud Technologie ist. CC basiert auf einer Hardwarestruktur und diese Hardware ist auch bereits seit längerem in unterschiedlichen Endpoints, wie Chips, integriert. Auf dem Handy haben wir womöglich alle eine CC-Enklave.

Frage: Reden wir hier auch von TPM?

[2] Antwort: Die Technologie ist ähnlich. Aber man muss berücksichtigen, dass es unterschiedliche Definitionen von CC gibt. Es ist eine Hardware-Technologie und keine Cloud-Technologie. Was sich in der jüngeren Vergangenheit verändert hat, ist, dass die Technologie auf den Servern gewisser Hyperscalers, insbesondere Microsoft Azure, zur Verfügung steht. Entsprechend können die Systeme auf die Technologie gebaut werden. Und in diesem Moment wird es zu einem Cloud-Thema, weil dann steht der Server in einem Rechenzentrum eines Cloud-Providers. Dort siedelt sich die gegebene Problematik an.

Frage: Wieso führt die Bearbeitung von personenbezogenen Daten in der Cloud zu so vielen Diskussionen?

[3] Antwort: Vieles ist psychologisch und hat mit Recht nur im Ansatz etwas zu tun. Es werden in diesem Kontext auch viele Themen vermischt. So wird bspw. die Frage der grenzüberschreitenden Datenübermittlung oft vermischt mit der Cloud Act Thematik, wobei diese zwei Themen einen ganz anderen Sachverhalt regeln. Cloud Act regelt den Sachverhalt, wo die Daten die Grenze noch gar nicht überschritten haben und von Behörden aus dem Ausland darauf Zugriff verlangt wird. Wir übermitteln dabei die Daten gar nicht mehr ins Ausland, sondern allenfalls an einen Anbieter innerhalb der Schweiz, welcher unter dem Zugriffbereich dieses Cloud Acts steht. Wir sind dabei somit noch nicht in einer grenzüberschreitenden Datenübermittlung gemäss Datenschutzrecht. In diesem Umfeld ist extrem viel Unsicherheit entstanden. Es gibt effektiv Personen, welche der Meinung sind, dass die Bearbeitung von personenbezogenen Daten im einem Cloud Datacenter gar nicht mehr möglich ist auf legalem Weg. Das kann man so

vertreten, wenn man gewisse Gesetze entsprechend auslegt. Wie bspw, das Schrems II-Urteil. Wenn man das sehr strikt auslegt, ist es möglicherweise tatsächlich so. Ich bin jedoch der Meinung, dass dies nicht der eigentliche Wille des Gesetzgebers war.
[4] Letztendlich geht es um die Frage, wohin gehen die Daten, wenn man sie einer Cloud überlässt. Gehen sie an einen Cloud Anbieter der die Daten in einem Staat bearbeitet, welcher kein angemessenes Datenschutzniveau gewährleistet, und wenn dem so ist, mit welchen Massnahmen kann man dem entgegenwirken. Eine dieser Massnahmen ist Verschlüsselung. Damit ist eine Verschlüsselung gemeint, bei der auf den Schlüssel im Land, dem man nicht vertraut, kein Zugriff möglich ist. Geht man davon aus, dass in einem Land, welchem man nicht vertraut, verschlüsselte Daten sind, und der Schlüssel im Land nicht zugreifbar ist, hat man das Vertrauensproblem gelöst. Man geht davon aus, dass die Daten in diesem Land gar nicht gelesen werden können. Der Lösungsansatz verhindert allerdings viele Nutzungsmöglichkeiten von Cloud Services. Mit traditioneller Technologie lassen sich so in der Cloud fast nur Anwendungsfälle der einfachen Datenspeicherung (*Storage*) umsetzen. Lade ich meine Daten auf einen Sharepoint, kann ich das verschlüsselt mit einem eigenen Schlüssel, den ich selbst kontrollieren und dafür sorgen kann, dass dieser nicht ins jeweilige Land gelangt. Das wäre eine mögliche zusätzliche technische Massnahme, in Ergänzung vertraglicher Massnahmen wie den EU-Standardvertragsklauseln (SCC), welche von der Schrems II Rechtsprechung gefordert wird. Sobald man jedoch mit den Daten auf der Cloud arbeiten möchte, lässt sich dieser vorhin genannte Lösungsansatz mit der Verschlüsselung zumindest mit traditioneller Technologie kaum mehr umsetzen. Genau an diesem Punkt setzt CC an. Die Analyse der Daten ist dabei ein Use Case, welcher Stand heute mit CC umsetzbar ist. Es ist noch nicht juristisch beleuchtet, aber in Anbetracht dessen, was bisher zu technischen Massnahmen und Schrems II geschrieben wurde, wäre es eine logische Schlussfolgerung, dass bei einer Datenanalyse in einem CC-Umfeld der Belegenheitsort der Sever keine Rolle mehr spielt. Man kontrolliert die Versschlüsselung. Wo die auf diese Weise verschlüsselten Daten liegen, ist dann rechtlich unerheblich. Vermutlich werden zusätzlich zur Datenanalyse immer mehr Use Cases dazu kommen. Je leistungsfähiger die Hardware, desto mehr Use Cases lassen sich wohl mit der Zeit realisieren mit CC. Dort müsste die Art der Verschlüsselung den Anforderungen einer sehr strikten Auslegung vom Schrems II-Urteil genügen.

Frage: Kurze Zwischenfrage, wurde Schrems II nicht für ungültig erklärt?

[5] Antwort: Nein. Schrems II kann man nicht für ungültig erklären. Schrems II ist ein Urteil vom EuGh. Was sicherlich der Fall ist, dass vieles, was über Schrems II geschrieben wurde, nicht stimmt. Es wird oft geschrieben, dass Schrems II die SCC der Europäischen Kommission für ungültig erklärt. Das stimmt so nicht. Es wird lediglich in einem Nebensatz erwähnt, dass selbst wenn man die SCC nutzt für die Übermittlung von personenbezogenen Daten in die USA oder andere unsichere Drittstaaten, man sich nicht mehr eifach auf den Abschluss der SCC verlassen kann. Zusätzlich zu den SCC muss man eine Risikoanalyse durchführen (Transfer Impact Assessement, TIA). Wenn man im Rahmen dieses TIAs zum Schluss kommt, dass die SCC nicht ausreichen, dann muss man zusätzliche Massnahmen ergreifen, um einen angemessenen Schutz der übermittelten Daten zu gewährleisten. Dort würde die Verschlüsselung anhand eines proprietären Schlüssels im eigenen Land oder innerhalb von sichern Staaten das Problem lösen. Das ist das eine.

[6] Nebst den SCC hatte man bis zum Schrems II Urteil die Möglichkeit, Daten in ein Drittland zu übermitteln, sofern der Empfänger nach einem bestimmten Mechanismus zertifiziert oder selbstzertifiziert war. Im Falle der USA sind die Anforderungen an eine solche Zertifizierung im sogenannten Privacy Shield Framework abgebildet. Auch das Privacy Shield Framework wurde entgegen der von vielen vertretenen Auffassung nicht für ungültig erklärt. Jedoch der Beschluss, wonach Privacy Shield für einen ausreichend Schutz sorgt, ist für nichtig erklärt worden. Das heisst, Privacy Shield gibt es heute noch und ist in den letzten Zügen der Revision. Man kann davon ausgehen, dass sich Herr Schrems nach Inkrafttreten wieder einschalten wird und es ein Schrems III gibt. Das Problem liegt nämlich an einem anderen Ort. Kein Framework wird das eigentliche Problem lösen. Genau das gleiche Thema haben wir bei den SCC. Die Ausgangs-These, dass man diese SCC vereinbaren kann und anschliessend abgesichert ist, war wohl von Anfang an falsch. Man muss trotzdem stets überprüfen, ob nach diesem SCC gelebt und das auch umgesetzt werden kann.

[7] Wenn im Empfängerstaat eine Gesetzgebung vorhanden ist, welche beispielsweise den örtlichen Geheimdiensten weitreichende und nach Europäischer Auffassung nur ungenügend rechtstaatlich legitimierte Kompetenzen einräumt, kommen Empfänger von Personendaten in solchen Staaten möglicherweise in die Situation, wo sie sich entscheiden müssen zwischen der Verletzung der SCC oder der Verletzung der betroffenen Gesetzesbestimmungen. Die Annahme des EuGH ist, dass sich ein Datenempfänger in einer solchen Situation wohl eher dazu entscheiden würde, die SCCs zu verletzen als sich

auf eine Konfrontation mit den lokalen Geheimdiensten einzulassen. Die Durchsetzbarkeit der SCC ist somit in Frage gestellt. Dort liegt das eigentliche Problem. Nachher gibt es unterschiedliche Auslegungen dazu, was ein angemessenes TIA ist. Folgt man einer strengen Auslegung, darf man grundsätzlich keine Personendaten mehr in Länder übermitteln, deren Gesetzgebung möglicherweise die Durchsetzbarkeit der SCC verunmöglicht. Eine Übermittlung von Personendaten in solche Staaten ist dann nur noch zulässig, wenn man neben vertraglichen Massnahmen wie den SCC zusätzliche technische Massnahmen wie Verschlüsselung trifft, welche den Datenzugriff auf technischer Ebene verunmöglichen. Wenn man Schrems II so auslegt, kann man Stand heute für die meisten Anwendungsfälle mit traditionellen Mitteln keine Personendaten mehr in die USA übermitteln. Einzige Ausnahme bilden dann Datenübermittlungen für sehr banale Anwendungsfälle wie die reine Datenspeicherung.

[8] Es gibt allerdings auch einen Ansatz, der besagt, dass zusätzlich die Eintretenswahrscheinlichkeit berücksichtig werden muss. Dabei geht es darum, ob effektiv eine gewisse Wahrscheinlichkeit besteht, dass der Datenempfänger in den vorhin erwähnten Konflikt zwischen Verletzung der SCC oder Verletzung der lokalen Gesetzgebung kommen wird. Dabei ist namentlich von Bedeutung, ob Geheimdienste eines Empfängerstaates überhaupt Interesse haben könnten an den Daten. Dort wird man regelmässig zum Schluss kommen, dass die betroffenen personenbezogenen Daten von keinerlei Interesse für Geheimdienste sind. Geheimdienste würden den Aufwand überhaupt nicht betreiben, um an solche Daten zu kommen. So einfach, wie es teilweise klingt, ist es nämlich gar nicht. Es benötigt viele Ressourcen und diese schöpft ein Geheimdienst nur aus, wenn ein reales Interesse besteht an den Informationen. Berücksichtigt man diese Tatsache in einer Risikoabwägung, verursachen beispielsweise allgemeine HR-Daten auf einem Cloud-System nicht mehr so ein grosses Risiko. David Rosenthal hat eine solche Methode entwickelt. Er hat ein strukturiertes Impact Assessement entwickelt, mit dem man die Wahrscheinlichkeit berücksichtigt und dann in vielen Use Cases zu einem Risiko von unter 10% oder in der Regel sogar in einem Bereich von 1% bis 5% gelangt. Dies ist nicht dem Umstand geschuldet, dass Rosenthal die Methode mit dem Ziel entwickelte, möglichst tiefe Werte zu generieren. Vielmehr ist es wohl eben tatsächlich so, dass sich Geheimdienste nicht für jede Information interessieren. Wenn man das intern dokumentiert, wird ersichtlich, dass es keinen begründeten Anlass gibt, davon auszugehen, dass eine Verletzung der Grundrechte der betroffenen Personen aufgrund der möglicherweise zu umfangreichen und zu wenig rechtstaatlich kontrollierten Kompetenzen

von Geheimdiensten wahrscheinlich ist. Die Frage, ob die Datenschutzgesetze im Empfängerstaat einen angemessenen Schutz gewährleisten ist eine andere.
[9] Risiken für die Grundrechte der betroffenen Personen, welche aus möglichen Unzulänglichkeiten oder gänzlichem Fehlen von Datenschutzgesetzen im Empfängerstaat resultieren, sucht man auf vertraglicher Ebene durch die SCC abzudecken. Dazu sind die SCC bestimmt, nicht um die betroffenen Personen vor dem Übereifer von Geheimdiensten zu schützen. Auf dieser Basis ist ein angemessener Schutz der betroffenen Personen gewährleistet. Entsprechend ist es erlaubt, die Daten zu übermitteln. Das ist der risikobasierte Ansatz. Dort haben die SCC weiterhin ihre Daseinsberechtigung und im Übrigen hat auch ein Privacy Shield Framework in diesem Bereich seine Daseinsberechtigung. Der Schutz und die Kontrolle, welche das Privacy Shield Framework und eine Zertifizierung unter Privacy Shield gewährleisten, ist dem, was man bei SCC vereinbart, sehr ähnlich. Es geht teilweise sogar noch weiter und ermöglicht teilweise noch einen effektiveren Schutz der betroffenen Personen, was ja das Kernanliegen des Datenschutzes ist. Dieses Kernanliegen des Datenschutzes geht in der öffentlichen Debatte leider teilweise abhanden. Nicht nur in der öffentlichen, sondern auch in der Diskussion unter Datenschutz-Spezialisten. Das ist dann meiner Meinung nach ein bisschen verantwortungslos, wenn man als Datenschutzexperte Extrempositionen einnimmt, ohne zu wissen, was denn die tatsächlichen Auswirkungen sind.
[10] Allerdings: Selbst wenn man von einer strengst möglichen und restriktiven Auslegung von Schrems II ausgeht, müsste CC die Datenübermittlung in die USA und andere Staaten ermöglichen, vorausgesetzt, dass es entsprechend aufgegleist ist, und dass, wie bereits erwähnt, die Kontrolle über den Schlüssel ausserhalb dieser Staaten bleibt.

Frage: Ändert CC etwas an der Datenschutzkonformität?

[11] Antwort: Datenschutzkonformität hängt von der einzelnen Datenbearbeitung ab. Die Frage, welche sich im Zusammenhang mit CC für mich stellt, ist, ob ich anhand von CC eine Datenbearbeitung, welche sonst nicht datenschutzkonform wäre, datenschutzkonform gestalten kann. Oder kann ich bei einer Datenbearbeitung, welche zwar datenschutzkonform ist, aber risikoreich wäre, das Datenschutzrisiko erheblich minimieren in dem ich CC einsetze. Der Einsatz einer Technologie kann für sich selbst nicht datenschutzkonform sein oder nicht, sondern es stellt sich die Frage, ob die Bearbeitung datenschutzkonform ist. Ein sehr wichtiger Punkt in der Beurteilung der Datenschutzkonformität eines Datenbearbeitungsvorgang ist das Treffen von angemessenen

technischen und organisatorischen Massnahmen zu Sicherstellung der Datensicherheit. Wenn ich mit CC arbeite, dann ist CC eine technische und im beschränkten Mass eine organisatorische Massnahme zur Gewährleistung der Datensicherheit. Zum einen werden die Daten verschlüsselt. Dadurch stelle ich die Vertraulichkeit der Daten in erhöhtem Mass sicher. Zugriff auf die Daten haben nur diejenigen, welche Zugriff auf den Schlüssel haben. Ein Teil der Unsicherheit der Cloud ist, dass, wenn man einen Cloud Provider einsetzt und auf dessen Infrastruktur Daten bearbeitet werden, bspw. in Form einer Analyse oder das Abspeichern von Daten, das Senden und Empfangen von E-Mails etc., dann funktioniert das nur, wenn das System des Anbieters die Daten lesen kann. In diesen Fällen wird es in aller Regel beim Anbieter irgendeine Person oder Personengruppe (i.d.R. Administratoren) geben, welche die Berechtigung besitzt, sämtliche Schutzmechanismen zu durchbrechen und auf die Daten zuzugreifen. Zwar wird man als Nutzer dieser Dienste, wenn man sorgfältig agiert, Verträge haben, welche dem Anbieter verbieten, auf die Daten zuzugreifen oder das zumindest auf eine sehr limitierte Anzahl von Szenarien (beispielsweise, wenn ein Zugriff auf Klardaten im Rahmen des Supports notwendig ist) beschränken.

[12] Weiter gibt es organisatorische Massnahme, so dass beispielsweise ein Mitarbeiter eines Providers, welcher böswillige Absichten hegt, kann nicht allein handeln kann. Innerhalb des organisatorischen Setups eines Providers müssen dann mindestens zwei Personen zusammenarbeiten, damit die Daten im Klartext eingesehen werden können. Die Massnahmen sind insbesondere bei grossen und sehr professionell aufgestellten Anbietern oftmals sehr ausgeklügelt, sodass diese zwei Personen beispielsweise im Voraus voneinander nicht wissen, wer sie sind. Die zweite Person wird per Zufallsprinzip ausgesucht. Das heisst, diese zwei Personen können keinen Angriff zusammen planen.

[13] Trotz all dieser Massnahmen hat man aber im Prinzip immer das Risiko, dass ein Super-Administrator die Daten trotzdem einsehen kann. Diesem Risiko sind sich auch die Anbieter bewusst und liessen sich sehr vieles einfallen, damit bei der Kundschaft Vertrauen aufgebaut wird.

[14] Ein wesentlicher Faktor bei CC ist die Eliminierung des vorhin dargelegten sogenannten Administratoren-Risikos. Nutzt man CC beispielsweise innerhalb einer Microsoft Umgebung, gibt es niemanden bei Microsoft, der auch nur theoretisch die Möglichkeit hätte, an die Schlüssel zu gelangen. Dadurch wird eine organisatorische Massnahme ersetzt, bei der man immer noch vertrauen muss, dass diese auch tatsächlich umgesetzt ist. Wenn man Daten in einer CC Umgebung innerhalb der Infrastruktur von

Microsoft bearbeitet, muss man Microsoft nicht vertrauen, sondern nur in die Technologie. Die Technologie kommt in diesem Falle von Intel und Intel wiederum kommt nicht in Kontakt mit den Daten. Sogar wenn Intel als Hardwarelieferant mit Microsoft als Cloud Anbieter zusammenarbeiten würde, hätten diese beiden Parteien zusammen wohl nicht die Möglichkeit auf die unverschlüsselten Daten zuzugreifen, wenn die zur Datenbearbeitung eingesetzte und auf CC aufbauende Software von einem Drittanbieter wie Decentriq kommt. Es bräuchte eine sehr komplexe konspirative Zusammenarbeit zwischen mehreren unabhängigen Parteien, um an die unverschlüsselten Daten zu gelangen. Man spricht daher oft davon, dass CC den sog. Vertrauensperimeter auf die kleinstmögliche Ebene herunterbricht. Das bedeutet, der Nutzer muss nur noch der Technologie vertrauen. Dann ersetze ich organisatorische Massnahmen, welche letztlich unzuverlässig sind, da Personen immer noch mehr können als sie dürfen, durch zuverlässigere technische Massnahmen. Mit CC können Personen gar nicht mehr, was sie nicht dürfen. Man hat eine sehr starke, technische Massnahme, welche die organisatorische Massnahme schlussendlich obsolet macht. Dort liegt der Vorteil.

[15] Man kann sich zum Beispiel Fälle vorstellen, bei denen das Hochladen von Daten in eine Cloud für einen Analytics Use Case ein besonders grosses Risiko darstellt, etwa weil die Daten besonders sensibel sind und/oder weil die Daten von mehreren Parteien zusammengeführt und gemeinsam ausgewertet werden. Man muss allen involvierten Parteien und Organisationen vertrauen. Überwiegt das Risiko den Nutzen, wird man sich gegen das Projekt entscheiden. Mit der technischen Massnahme von CC hat man hier allenfalls die Möglichkeit, das Risiko auf ein so kleines Niveau zu reduzieren, dass bei der Betrachtung desselben Use Case der Nutzen überwiegt.

Frage: Was verändert CC im Bereich der Datenbearbeitung? Kann jetzt die Datensicherheit bei der Bearbeitung von besonders schützenswerten Daten noch besser gewährleistet werden?

[16] Antwort: Schlussendlich liegt der Schlüssel bei der Datenbearbeitung. Es geht um technische und organisatorische Massnahmen und deren Angemessenheit. Das wichtige ist der Begriff der Angemessenheit. Diese orientiert sich am Schutzbedarf der jeweiligen Daten. Der Schutzbedarf ist bei den besonders schützenswerten Daten höher. Das bedeutet, dass für besonders schützenswerte Daten stärkere Massnahmen getroffen werden müssen. Das ist nie schwarz oder weiss. Ich bin der Meinung, dass CC etwas beeinflussen kann. Man muss dabei in Risikoszenarien denken. Bei den Gesundheitsdaten

denkt man direkt an die Vertraulichkeit. Daher hat man oft auch den Eindruck, dass die Datensicherheit nur mit Vertraulichkeit zu tun hat. Das stimmt aber nicht. Die Datensicherheit hat mehrere Vektoren und Datensicherheit ist nur einer davon. Bei besonders schützenswerten Daten steht jedoch die Vertraulichkeit tatsächlich oft im Vordergrund. Eine Vertraulichkeitsverletzung kann bspw. sein, dass jemand, der berechtigterweise Zugriff auf die Daten hat, etwas macht, was er nicht tun darf. Es kann auch ein externer Angreifer sein, welcher sich unberechtigt Zugriff zu den Daten verschafft und diese beispielsweise stiehlt. Nun gilt es, die wesentlichen Risiken der Vertraulichkeit zu eruieren und Massnahmen zu treffen, welche diese Risiken minimieren. Mit CC reduziert man die Anzahl der Personen, welche theoretisch Zugriff auf die Daten haben, obwohl dieser Zugriff nicht notwendig wäre. Das heisst auch, dass beispielsweise auch Cloud-Administratoren keinen Zugriff auf unverschlüsselte Daten mehr haben. Man hat somit plötzlich eine Massnahme, bei der man sich nicht nur zusichern lässt, welche organisatorischen Massnahmen der Provider trifft, wobei solche Zusicherungen natürlich immer auch verletzt werden können. Man benötigt das gar nicht mehr, denn dasselbe Schutzziel wird durch eine technische Massnahme erreicht, welche wie vorhin erläutert zusätzlich nur sehr schwer zu umgehen ist. Zurück zum Risikoszenario mit dem Angreifer ist es Tatsache, dass sich die modernsten Angriff-Szenarien offenbar immer mehr auf die Daten in Use konzentrieren. Mit CC schützt man die Daten in diesem Aggregatszustand. Das heisst, die technische Schutzmassnahme von CC bietet plötzlich einen Schutz, welcher durch traditionelle Verschlüsselungsmethoden nicht gewährleistet werden konnte. Man hat einen höheren Schutzstandard und kann somit eher rechtfertigen, dass die Schutzmassnahmen angemessen waren. Das ist der wohl offensichtlichste Vorteil von CC.

[18] Aus rechtlicher Perspektive finde ich jedoch fast noch interessanter, dass man innerhalb von CC-Lösungen umsetzen kann, welche nur bestimmte Berechnungen zulassen. Als Dateninhaber kann man entsprechend im Vorhinein in tiefster Granularität festlegen, zu welchen Zwecken die Daten bearbeitet werden dürfen. Nimmt man bspw. eine hypothetische Patientendatenbank und lässt ein Analyse Skript durchlaufen, kann ich sehen, welcher Output generiert wird. Ich kann mich davon vergewissern, dass der Output die Anforderungen an die Nicht-Re-Identifizierbarkeit der betroffenen Patienten erfüllt. Bspw., dass nur ein Output ausgegeben wird, wenn der Datensatz auf einem Datensatz von mehr als 100 Patienten beruht. Wenn es nur 99 sind, dann generiert die Lösung kein Analyse-Resultat, da die Ungewissheit der Re-Identifizierung bestehen

bleibt.[317] Als Herr über die Daten kann ich mich aufgrund des Analyse-Skripts darüber vergewissern, dass ich mit dem Output einverstanden bin. Sobald ich das gemacht habe, kann ich meine Daten innerhalb einer CC Umgebung an ein Pharma-Unternehmen oder an sonstige Forschungsinstitutionen bereitstellen und technisch gewährleisten, dass innerhalb der CC Umgebung einerseits nicht auf meine unverschlüsselten Daten zugegriffen werden kann und andererseits nur das von mir freigegebene Analyse-Skript ausgeführt werden kann. Die Vertraulichkeit der Patienten-Identität ist gewährleistet.
[19] Man kann sich zudem technisch attestieren lassen, dass nie ein anderes Skript innerhalb der CC Umgebung ausgeführt wurde. Es gibt eine umfangreiche Kontrolle darüber, was mit den Daten passiert oder passieren kann. Ich muss meine Daten zudem keinem Analytics-Unternehmen mittels eines Auftrags vertrauensbasiert überlassen. Vertrauen kann zwar wie vorhin besprochen auch mittels vertraglich zugesicherter organisatorischer Massnahmen geschaffen werden. Weiter kann Fehlverhalten mittels festgelegten Bussgeldern sanktioniert um so Abreize zu schaffen. Aber mit CC ist das eigentlich nicht mehr nötig. Ab dem Zeitpunkt, wo das Skript freigegeben wird in CC, weiss man, dass nichts anderes mit den Daten passieren kann, als das, was man im Voraus erlaubt hat. Aus Sicht der datenschutzrechtlichen Zweckbindung ist die Kontrolle mittels CC sehr viel effektiver. Der Verantwortliche hat die Kontrolle über die Datenbearbeitung. Das ist einer der grossen Vorteile von CC.

Frage: Würdest du als Datenschutzbeauftragter des Stadtspitals CC nutzen für eine Datenbearbeitung von besonders schützenswerten Personendaten?

[20] Antwort: Das ist eine komplexe Frage, da hier nicht nur das Datenschutzgesetz relevant ist. Die Use Cases, welche für ein Spital im Vordergrund stehen, sind das Zugänglichmachen der eigenen Daten zu Forschungszwecken. Als Spital würde ich die Daten meiner Patienten tatsächlich mit einem sehr viel besseren Gewissen freigeben, wenn ich wüsste, dass ich sie in ein CC-Umfeld hochlade, vorausgesetzt, ich weiss auch, wie letzteres im Detail aufgesetzt und konfiguriert ist. Man darf aber nicht vergessen, dass es beispielsweise auch noch das Humanforschungsgesetz gibt. Darin ist der Grundsatz der informationellen Selbstbestimmung sehr viel ausgeprägter reflektiert als in der Datenschutzgesetzgebung. Im Humanforschungsgesetz gibt es ausdrückliche

[317] Die Zahlen 100 und 99 dienen als Beispiel und sind frei gewählt. Ab welcher Anzahl von Personen man die Re-identifizierbarkeit ausschliessen kann, hängt von vielen verschiedenen Faktoren ab, die im vorliegenden Kontext nicht erläutert werden.

Einwilligungserfordernisse für gewisse Formen der Nutzung von medizinischen Daten von Patientinnen und Patienten für Forschungszwecke. Sobald ich von einem Patienten eine Einwilligung benötige, um seine Daten zu Forschungszwecken zu nutzen, steht die Vertraulichkeit der Daten nicht mehr einzig im Vordergrund. Bevor ich Daten eines Patienten für Forschungsprojekte freigebe, muss ich sicherstellen, dass ich eine Einwilligung habe für genau diesen Forschungszweck. Das kann in gewissen Fällen generisch sein (General Consent). In der Krebsforschung gibt es ausserdem noch das Krebsregister-Gesetz. Je nach Forschungsprojekt hat man es mit einem komplexen Gewebe von unterschiedlichen und sich überlagernden Gesetzesnormen zu tun. Dazu kommen auch noch kantonale Datenschutzgesetze, welche für öffentliche und teilweise auch private Spitäler massgebend sind.

[21] In einem kürzlich publizierten Gutachten kommt die Anwaltskanzlei Meyerlustenberger Lachenal (MLL) sodann zum Schluss, dass es mit der heutigen fragmentierten Gesetzgebung in der Schweiz beinahe unmöglich ist, Gesundheitsdaten für Sekundärzwecke zu nutzen. Es ist für Entscheidungsträger schlicht nicht möglich, die rechtlichen Risiken angemessen zu beurteilen. Es wurde in diesem Gutachten aber auch geschrieben, dass einige der Probleme der Sekundärnutzung von Gesundheitsdaten in der Schweiz durch Confidential Computing möglicherweise lösbar wären. Nun müsste man analysieren, wie man die Risiken, welche im Gutachten erwähnt werden, minimieren kann mit CC. Dort spielt einerseits die Sicherstellung der Vertraulichkeit der Daten eine wichtige Rolle. Noch wichtiger ist, dass ein Spital die Kontrolle über die Daten behält. Es gibt verschiedene innerhalb einer CC Anwendung umsetzbare Ansätze, um dies zu gewährleisten. Diese Ansätze rechtlich zu validieren, ist nun die Herausforderung.

Ende des Experteninterviews.

Transkript 4

Experteninterview mit Lucian Hunger, Rechtsanwalt

Frage: Welche Fragestellungen begegnen Ihnen im beruflichen Alltag im Bereich der Cloud-Technologie oder allgemein Technologien in Zusammenhang mit den rechtlichen Anforderungen?

[1] Antwort: Es kommt darauf an, wer die Frage stellt. Im Berufs- oder Amtsgeheimnisbereich geht es um den Einsatz und die Umsetzung. Die anfragenden Kunden kommen mit der Absicht, in die Cloud zu migrieren. Dabei beantworten wir Fragestellungen zu den Verträgen und zur Umsetzung. Bei den kleineren Kunden kommen häufiger allgemeine Fragen im Bereich der Umsetzung. Dabei stellt sich die Frage, wie man etwas möglichst gut umsetzt, es aber praktikabel bleibt. Unseren Klienten müssen auch wissen, dass es im Datenschutz nicht möglich ist alles zu erfüllen. Man muss einen risikobasierten Ansatz verfolgen.

Frage: Welche praktikablen Überlegungen muss sich ein Unternehmen machen, resp. welchen risikobasierten Ansatz wählt man, wenn eine Datenbearbeitung mit einer technischen Lösung datenschutzkonform umgesetzt werden soll?

[2] Antwort: Ich habe sehr viele Cloud-Projekte im Bereich der Berufsgeheimnisse, sprich Bankgeheimnis, Arztgeheimnis, öffentliche Institutionen etc. Wir haben dafür ein Cloud Compliance- und Risk-Assessment-Tool entwickelt. Dies ist für öffentliche Institutionen wie bspw. Spitäler und Behörden, welche unter dem Amtsgeheimnis stehen, frei zugänglich. In diesem Assessement geht es darum, sich bewusst zu sein, was man wie macht. Man muss dokumentieren, welche Abhängigkeiten bestehen, welche Daten bearbeitet werden, welche Art von Datenbearbeitung in der Cloud geschieht. Die Frage ist schlussendlich, ob die Migration in die Cloud das Ziel ist oder ob wir den Fokus auf die Datenbearbeitung legen. Grundsätzlich ist die Datenbearbeitung bereits geklärt i.S.v. man darf diese Daten bearbeiten. Das zusätzliche Risiko besteht also in der Migration in die Cloud. Wir führen also mittels unterschiedlicher Prüfprogramme eine umfangreiche Beurteilung durch. Der rechtliche Part stellt dabei nur einen Teil dar. Es handelt es sich um eine interdisziplinäre Angelegenheit. Wir führen solche Beurteilungen jedoch in der Regel für grössere Kunden durch (Spital, Bank etc.), und selten für KMU. Involviert sind dabei Projektbereiche wie CISO, DPO, IT, Legal und eine Projektleitung, welche das ganze steuert. Jedes Team trägt dabei die fachspezifische Verantwortung. Das Legal

Team untersucht, ob die Verträge in Ordnung sind. Der DPO kümmert sich um datenschutzrechtliche Aspekte. Die IT klärt unter anderem zusammen mit dem CISO die (Sicherheits-)Einstellungen.
[3] Die Richtigkeit dieser Einstellungen beurteilen dann nicht wir, sondern andere Spezialisten. Unsererseits wird dann gefragt, ob etwas gemacht wurde, ob ein Konzept vorhanden ist und ob sie wissen, wie vorzugehen ist. In diesem Assessement gibt es dann ganz viele Folgefragen. Für die KMU haben David Rosenthal und David Vasella die sechs Faustregeln veröffentlicht. Es geht insbesondere darum, dass man daran denkt, eine ADV abzuschliessen, und wenn möglich mit einem europäischen Unternehmen (kann auch ein europäisches Tochterunternehmen sein) den Vertrag abschliesst. Das ist ein Aspekt, woran sich Schweizer Unternehmen noch dran gewöhnen müssen. Im Bereich der DSGVO ist das bereits gängig. Das muss man sicher im Griff haben. Bei der Cloud sind auch insbesondere die folgenden zwei Aspekte zu berücksichtigen: Wie wird die Cloud konfiguriert und die Durchführung eines eigenen Backups. Ein Backup hängt insofern mit dem Datenschutz zusammen, dass man die Verfügbarkeit und Integrität gewährleisten muss aber das Durchführen eines Backups hat auch unternehmerische Gründe. Eine Cloud ist in der Regel kein Backup und darüber bestehen häufig Fehlauffassungen.

Frage: Bei welcher Art von Daten spielt der Standort des Providers noch eine Rolle?
[4] Antwort: Dies Aspekt müssen wird differenziert betrachten. Wir haben einerseits den Vertragspartner, welcher, unabhängig des Serverstandortes, entweder in der Schweiz oder im EWR sein sollte. Das hat aus der Lawful Access Optik seine Vorteile. So hat man als Kunde keinen direkten Vertrag mit einem Unternehmen aus den USA. Im Lawful Access wird risikobasiert die Wahrscheinlichkeit eines Datenzugriffs durch den ausländischen Staat (z.B. USA) beurteilt. Wenn man nun Kunde ist von einem europäischen Unternehmen, welches eine Tochtergesellschaft eines amerikanischen Unternehmens ist, dann kann man sich vom amerikanischen Unternehmen abgrenzen, da man vertraglich nicht direkt Kunde ist. Man muss sich aber bewusst sein, dass man das Risiko nicht gänzlich eliminiert, solange eine amerikanische Muttergesellschaft hinter der Tochtergesellschaft aus der Schweiz oder dem EWR ist. Beim Speicherort geht es insbesondere um den Art. 271 StGB. Ich mache ein Beispiel. Die Mitarbeiter eines Cloud-Anbieters in der Schweiz geben Daten an den amerikanischen Staat heraus und können sich somit strafbar nach Art. 271 StGB machen. In der Regel wird dieses Argument von

amerikanischen Gerichten akzeptiert. Wie bei jeder Anfrage zur Datenherausgabe muss man sich fragen, wie gross die Gewinnchancen vor Gericht sind und welche Argumente man hat, damit man die Daten nicht herausgeben muss. Also, d.h. ich habe das Argument, dass meine Mitarbeiter sich strafbar machen, wenn sie die Daten herausgeben. Dies ist ein starkes Argument, dass Erfolg bringen kann.

Frage: Ist das Risiko abhängig von der Art der Daten und deren Schutzbedarf?

[5] Antwort: Dort geht es vor allem darum, wann eine grosse Wahrscheinlichkeit bestehen könnte, dass ein Staat versucht Zugriff auf die Daten zu erlangen. Das müssen nicht unbedingt besonders schützenswerte Daten sein. Es wird dabei bspw. die Kommunikation mittels Key Words analysiert, ob diese an eine Zielperson gerichtet ist. In welchen Fällen passiert das nun. Das Risiko ist bei Geschäftsdaten viel kleiner als bei Kommunikationsdaten, da die Key Words nicht auf den Inhalt der Kommunikation, sondern darauf reagieren, an wen sich die Kommunikation richten. Das ist ein relevanter Punkt. Natürlich ist aber auch der Schutzbedarf der Daten zu berücksichtigen. Je höher dieser ist, desto besser sollten diese geschützt sein. Je sensibler die Daten sind, desto besser ist es, wenn diese in der Schweiz sind.

Frage: Wie fortschrittlich ist die Digitalisierung im Gesundheitsbereich?

[6] Antwort: An vielen Orten wird nun M365 eingeführt, aber in der Regel noch nicht für die besonders schützenswerten Patientendaten. Viele sind eher noch am Anfang, ausser evtl. im Startup-Bereich.

Frage: Welche Use Cases sehen Sie für den Einsatz von Confidential Computing (CC) im Gesundheitsbereich?

[7] Antwort: Ich sehe nicht, dass es ein Use Case wird, um die Daten innerhalb einer Cloud zu schützen. Mit CC haben wir die Möglichkeit, die Daten in den Datenräumen mit spezifisch definierten Codes zu bearbeiten. Das heisst, für ein Patientendossier ist das gemäss meinem Verständnis nicht relevant. Das wird somit nicht in erster Linie ein Anwendungsfall sein. Ich sehe es in der Zusammenarbeit zwischen einem Spital und einem Pharmaunternehmen. Die Patientendaten können ohne den Zugriff des Pharmaunternehmens und ohne den Zugriff von Dritten in diesem Datenraum bearbeitet werden.

Frage: Sehen sie noch einen anderen Anwendungsfall?

[8] Antwort: Nebst der Forschung und Statistik sehe ich die Nutzung auch im Bereich des Marketings. Zwei Unternehmen können durch die Nutzung die Insights aus ihren Kundendaten evaluieren, ohne, dass die andere Partei einen Zugriff auf die Kundendaten erhält.

Frage: Wie kann der Kunde als Controller die Integrität von einer Technologie, resp. die Bearbeitung durch den Auftragsbearbeiter prüfen und im Sinne der Datenschutzkonformität beweisen?

[9.1] Antwort: Das ist eine gute Frage. Wir haben das in unserem Excel auch aufgenommen. Bei den Grossunternehmen wird das vor allem über die SOC 2-Berichte oder über Zertifizierungen und externe Auditberichte abgewickelt. Intern muss man allerdings das Wissen sowie Kapazitäten Prozesse haben, dass es wiederum geprüft wird. Nur weil man den Bericht erhält, ist es ja noch nicht geprüft.

Frage: Wie stellt man sicher, dass diese Prozesse auch gelebt werden?

[9.2] Antwort: Dazu kann ich dir keine genaue Antwort geben. Aber das gibt es auch wieder externe namhafte Auditoren, welche die Prozesse überprüfen. Diese externe Auditberichte werden dann anschliessend auch von den Kunden geprüft, welche die Lösung einsetzen.

Frage: Zusammengefasst kann man also sagen, dass man bei einer Datenbearbeitung den Kontext sowie die Risiken, welche sich durch die Datenbearbeitung ergeben, berücksichtigen muss?

[10] Antwort: Aus datenschutzrechtlicher Sicht ist natürlich der Zweck der Datenbearbeitung auch relevant. Möchte man in eine Cloud migrieren, hat im Prinzip der Zweck nichts mit der Cloud zu tun. In der Regel wird durch die Nutzung einer Cloud die Verfügbarkeit und die Datensicherheit erhöht, da bspw. Microsoft viel mehr Kapazität hat. Natürlich geht man dabei andere Risiken wiederum ein wie der Lawful Access oder gewisse Abhängigkeiten. Wie geht es bspw. weiter, wenn es das Angebot nicht mehr gibt oder es sich verändert, der Vertrag sich ändert, neue Funktionalitäten erscheinen. Das muss man als Auftraggeber intern alles im Griff haben und Kontrollen durchführen. Früher konnte man diese Kontrolle noch im Serverraum selbst druchführen. Heute muss man einen SOC-Bericht überprüfen und einem Dritten vertrauen.

Frage: Können Sie den Hintergrund des Lawful Access nochmals erläutern?

[11] Antwort: Es geht darum, ob ein ausländischer Staat oder der Schweizer Staat auf Daten zugreifen kann. Ein Schweizer Staatsanwalt kann bspw. eine Verfügung erlassen, damit ein Schweizer Provider die Daten herausgibt. Die Frage ist, ob im Ausland ein Rechtsweg und ein Rechtssystem existieren, welcher demjenigen der Schweiz ähnlich ist oder ob Zugriffe möglich sind, die bei uns für den Staat unzulässig wären.. Es gibt bspw. die Abhörung der Internet-Backbones, welche man einfach beheben kann mit technischen Massnahmen, indem die Daten während dem Transport verschlüsselt werden. Das Risiko eines fremden Zugriffs ist in diesem Fall gering. Das kann so weit gehen, dass gemäss 702 FISA der amerikanische Staat verlangen kann, dass der Provider die Daten herausgeben muss, unter der Voraussetzung das der Provider «Possession, Custody or Control» über die Daten hat. Man kann mit technischen und organisatorischen Massnahmen die Datenbearbeitung so ausgestalten, dass dies verneint werden kann.
[12] Technisch kann man den z.B. den Zugriff des Providers auf die Daten verunmöglichen, in dem die Daten verschlüsselt werden. In der Realität ist das aber gewöhnlich nicht gänzlich umsetzbar. Der Provider braucht einen Schlüssel, damit er die Cloud-Dienstleistung erbringen kann. Es handelt sich somit um einen theoretischen Zugriff, welcher nicht täglich genutzt wird. Vor Gericht kann anhand dieser Argumentation die Herausgabe der Daten zurückgewiesen werden. Man muss dabei aufzeigen, wie das Unternehmen organisiert ist und warum man der Ansicht ist, nicht über «Possession, Custody or Control» zu verfügen. Ist man bspw. so organsiert, dass die Mitarbeitenden nur auf die Daten zugreifen können, sofern sie ein Approval seitens des Kunden erhalten haben, dann bedeutet dies, dass der Zugriff mittels einer organisatorischen Massnahme eingeschränkt wird und kein Control über die Daten besteht (kein Zugriff im täglichen Geschäft, sondern nur im Ausnahmefall).

Frage: Ist es eine Möglichkeit, dass vermehrt durch den Einsatz von technischen Massnahmen organisatorische Massnahmen reduziert werden?
[13] Antwort: Ja, es geht in diese Richtung. Das fängt bereits bei der automatischen Erinnerung zur Passwortänderung oder der Einführung von strikteren Passwortrichtlinien an.
Wir machen einen Blick in die Zukunft. Was sehen Sie als zukünftige Herausforderung in der Datenbearbeitung an?

[14] Antwort: Momentan reden alle über künstliche Intelligenz. Da sind noch viele Fragen zum Umgang ungeklärt.
Ende des Experteninterviews.

Transkript 5

Experteninterview mit Rehana Harasgama, Rechtsanwältin

Frage: Mit welchen Fragen sind Sie im beruflichen Alltag im Bereich der Cloud-Nutzung konfrontiert?

[1] Antwort: Es kommt darauf an, wer anfragt. Auf der einen Seite ist die Migration in die Microsoft Cloud 365 ein Thema bei uns im Bereich des Berufsgeheimnisses, insbesondere das Anwaltsgeheimnis. Das war bereits vor dem Schrems II-Urteil ein Fokus von uns. Es gibt Gutachten von anderen Kanzleien, welche das nicht so problematisch betrachten. Aber wir betrachten es aus der Perspektive des Berufsgeheimnisses, nicht speziell aus Sicht des Datenschutzgesetzes. Alle Bereiche, welche speziell reguliert sind wie zum Beispiel das Anwaltsgeheimnis, das Arztgeheimnis oder Bankkundengeheimnis haben Vorrang.

[2] Bei uns kam aber damals bereits der Cloud Act auf. Gerade, wenn man Daten von Klienten hat, welche Exposure in den USA haben, muss man aufpassen. Deswegen haben wir eine spezifische AGB mit Microsoft vereinbart. Das Vertragswerk von Microsoft ist sehr komplex. Inwiefern sich ihre Prozesse ändern, wenn man ein Addendum macht hinsichtlich des Anwaltsgeheimnisses, ist mir nicht so ganz klar, aber Microsoft ist ja in dieser Hinsicht sehr vorbildlich. Bei Ärzten habe ich die Erfahrung gemacht, dass viele ihre Daten bereits bei einem lokalen Anbieter speichern, was das Ganze ein bisschen einfacher gestaltet.

[3] Auf der anderen Seite haben wir Anfragen von Cloud-Anbietern, welche die Rechtslage verstehen möchten. Dort sind die Fragen sehr detailliert einerseits hinsichtlich der Angebote für Private. Es gibt auch sehr viele Fragen für Angebote für Behörden. Da spielt das kantonale Gesetz dann auch eine Rolle. Behörden und Bereiche, welche dem Amtsgeheimnis und Berufsgeheimnis unterliegen sind sich den Risiken sehr bewusst. Dieses Bewusstsein ist aber auch bei den Anbietern gestiegen. Die Provider versuchen, anstatt nur ihre Standardprodukt anzubieten, auch individuell Lösungen zu finden und werden sich immer mehr über die Komplexität des Themas bewusst. Gesetzliche Grundlagen sind sehr weit gefasst und es kommt immer auf die Art der Daten an, welche bearbeitet werden. Da muss man dann einen risikobasierten Ansatz wählen.

Frage: Wie ist das Risiko der Exposure bei Gesundheitsdaten?

[3] Antwort: Ich persönlich finde ja den Schrems-Entscheid nicht so förderlich. Aus Klienten-Sicht ist es nicht praktikabel. Ich sage nie, dass man keinen amerikanischen Anbieter wählen soll. Ich weise jedoch immer auf die Risiken hin, dass basierend auf den amerikanischen Gesetzesgrundlagen auf die Daten zugegriffen werden könnte. Es ist aber so, dass die grossen Cloud-Anbieter, welche einen gewissen Sicherheitsstandard gewährleisten, amerikanische Anbieter sind. Auf Seiten der Datensicherheit haben diese Anbieter eine sehr gute Voraussetzung. Das bedeutet aber nicht, dass kleinere Schweizer oder europäische Anbieter da nicht mithalten können. Aber da fehlt evtl. auch momentan noch die Erfahrung. Wichtig ist, dass auf die Risiken hingewiesen wird und man geeignete technische Massnahmen einsetzt, damit man die Risiken minimieren kann. Ganz eliminieren kann man sie nicht, ausser man wählt einen Schweizer oder europäischen Anbieter. Man muss jedoch auch klar sagen, dass die amerikanische Cloud-Thematik jetzt zu einem grossen Problem gemacht wird, da es alle betrifft. Über das Risiko weiss man meiner Meinung nach aber schon längst Bescheid. Der Schrems-Entscheid schafft jedoch auch Bewusstsein über die Problematik.
[4] Hinsichtlich der Art der Daten ist es klar, dass man Gesundheitsdaten von anderen Daten unterscheiden muss. Gesundheitsdaten haben einen höheren Schutzbedarf und da muss man sich überlegen, ob man diese in eine Cloud hochladen möchte. Ob diese für amerikanische Behörden interessant sind, ist dabei nicht die zentrale Frage. Gesundheitsdaten sind sehr intim und persönlich. Da geht es meiner Meinung nach auch um einen Daten-Ethik-Aspekt.
Frage: Gibt es immer ein Risiko, wenn der Konzern am Ende der Kette amerikanisch ist?
[5] Antwort: Auch wenn die Serverstandorte in der Schweiz oder in Europa sind und es sich um eine 100-prozentige Tochtergesellschaft handelt, hat man ein Risiko, wenn die Mutter in den USA ist. Man muss aber auch berücksichtigen, dass auch die Schweiz in einem Strafverfahren auf die Daten zugreifen kann. Der Unterschied zu den USA ist, dass keine datenschutzrechtlichen Grundsätze eingehalten werden müssen und die Datenherausgabe oft sehr unverhältnismässig sein kann. In der Schweiz kann die Polizei nur sehr beschränkt handeln in diesem Bereich.

Frage: Wie muss eine Datenbearbeitung datenschutzkonform ausgestaltet werden?
[6] Antwort: Wir sagen den Klienten immer, dass sie zuerst eine Due Diligence des potenziellen Anbieters durchführen sollen. Da geht es unter anderem um das Einholen von

Policies zur Datensicherheit und Access Management, Infos zu den Serverstandorten, Zugriffsregelung des Anbieters etc. Es geht bei der Beantwortung dieser Fragen darum, den Anbieter zu verstehen. Das ist meistens gar nicht so einfach. Viele Klienten fragen sich auch, wieso sie solche Aspekte überprüfen müssen, wenn bereits so viele andere die Dienstleistung nutzen. In der Beurteilung werden dann auch die technischen und organisatorischen Massnahmen angeschaut, welche aus rechtlicher Perspektive geprüft werden. Das beinhaltet Zugriffskontrollen, Transfer-Kontrollen, resp. alle Grundsätze, welche durch das Datenschutzgesetz gedeckt werden. Der Stand der Technik muss ein IT-Berater beurteilen. Wenn man während der Überprüfung feststellt, dass die Server unterschiedliche Standort haben, sollten unterschiedliche Optionen geprüft werden. Zu beachten ist in diesem Zusammenhang auch, dass Cloud-Provider oftmals auch Sub-Processors unter Vertrag haben. Da liegt genau das Risiko des Outsourcings. Man gibt die Kontrolle ab. In einem nächsten Schritt betrachtet man die Art der Daten, in welcher Form diese ausgelagert werden sollen und ob spezifische Gesetzesgrundlagen gelten, wie bspw. beim Berufsgeheimnis. Zudem müssen die eigenen Kundenverträge betrachtet werden. Dort können auch Auflagen bzgl. der Datenbearbeitung vorhanden sein. Danach gilt es, die notwendigen Verträge zu erstellen. Dazu gehören das Data Processing Agreement und wenn die Daten ins Ausland gehen zusätzlich das Data Transfer Impact Assessement. Zudem versucht man, zusätzliche technische Massnahmen einzuführen. Man geht vertraglich mehr Pflichten ein wie früher. Die Pflichten sind jedoch mittlerweile organisatorisch mit den Standard Contractual Clauses (SCC) sehr gut abgedeckt. Microsoft hat standardmässig bereits SCC und eine Auftragsdatenbearbeitungsvertrag (ADV), da sie von sich aus sagen, dass sie Processor sind.

[7] Die technische Seite war nicht immer sehr praktikabel. Die Guidelines des EDÖB beinhalteten die Bring your Own Key Encryption (BYOK). Das funktioniert, wenn es nur um die Speicherung der Daten geht. Für alles weitere ist dieser Ansatz nicht praktikabel. Da muss man andere Lösungen finden. Damit man die Risiken einschätzen kann, muss man einen für sich gangbaren Weg gehen. Das kann einerseits durch den risikobasierten Ansatz von Rosenthal passieren. Dieser ist jedoch nicht für jeden selbsterklärend und sehr komplex. Nebst den inländischen Risiken muss man bei Bedarf auch die ausländischen Rechtsgrundlagen prüfen. Da lohnt es sich, einheimische Anwälte beizuziehen.

Frage: Sollte man grundsätzlich bei Branchen mit Berufsgeheimnis davon absehen, Daten in einer amerikanischen Cloud zu bearbeiten?

[8] Antwort: Ich würde es nicht so sagen. Man muss den Personen die Risiken vor Augen führen. Der Entscheid fällt schlussendlich der Klient selbst. Unternehmen müssen sich auch bewusst sein, dass Grossanbieter wie Microsoft, AWS oder Google offen sind für Verhandlungen. Diese Anbieter sind sich den Problemen bewusst und haben bereits entsprechende Lösungen. Diese sind jedoch nicht Bestandteil der Standardlösung.

[9] Oftmals ist das Knowhow über die technischen Möglichkeiten bspw. in Spitäler nicht vorhanden. Ich bin aber immer wieder überrascht, wie aktiv die FINMA ist in diesem Bereich und informiert, was man darf und was verboten ist. Bei Gesundheitsdaten haben wir das Gegenteil, was den Rahmen für Beurteilungen sehr gross macht. Gleichzeitig hat jedoch die amerikanische Rechtsgrundlage mit dem Cloud Act, welche einen potenziellen Zugriff auf Daten erlaubt, das Risiko für die Datenbearbeitung in einer amerikanischen Cloud erhöht.

Frage: Confidential Computing verhindert durch eine technische Massnahme den Zugriff für sämtliche Beteiligte. Sehen Sie in dieser Technologie eine Chance, dass man eine gewisse *Datensicherheit für Daten ermöglichen kann, für welche dies vorher nicht möglich war?*

[10] Antwort: Ich glaube, dass man momentan die Hoffnung hat, dass es eine Chance ist, die Datensicherheit und datenschutzkonforme Nutzung zu nutzen. Aus rechtlicher Sicht besteht womöglich noch zu wenig Bewusstsein und Knowhow. Das könnte sich mit konkreten Use Cases ändern. Wenn man mit dieser Lösung tatsächlich alle Zugriffe verhindert, wäre das super. Wir haben schon oft diskutiert, dass es keine rechtliche Lösung gibt für das US-Problem. Ich bin der Meinung, dass man das technisch lösen muss.

Frage: Gibt es somit zukünftig mehr technische als organisatorische Massnahmen?

[11] Antwort: Bei den organisatorischen Massnahmen hat man immer den Faktor Mensch miteinbezogen. Man kann nur vertrauen, dass die Prozesse entsprechend umgesetzt werden. Die Hoffnung ist wohl, dass eine technische Massnahme einwandfreier funktioniert.

Frage: Wie kann ich eine technischen Massnahme auf ihre Integrität prüfen?

[12] Antwort: Ich denke, der Schlüssel ist der Beizug von unabhängigen IT-Auditors. Es ist aber immer sehr schwierig, diese Audits durchzusetzen. Am Schluss muss man Vertrauen in den Anbieter haben. Das ist zwischenzeitlich ein bisschen eingebrochen und muss wieder mehr aufgebaut werden. Vertrauen kann jedoch auch durch Empfehlungen und Richtlinien der Aufsichtsbehörden geschafft werden. Man liest zu oft, was man nicht darf, dabei fehlen einfach die Guidelines, welche aufzeigen, was man darf.
Ende des Experteninterviews.

Transkript 6

Experteninterview mit einem Rechtsanwalt (anonym)

Frage: Ist Confidential Computing (CC) in Ihrem Unternehmen ein Thema?

[1] Antwort: Es wäre falsch, wenn es kein Thema wäre. Es wäre bei jedem Unternehmen falsch, etwas anderes zu sagen, völlig unabhängig vom Inkrafttreten des neuen Datenschutzgesetzes. Es ist ein wichtiger Aspekt, wenn man Privacy oder den gesamten Datenumgang sowie den technikaffinen Aspekt einer Dienstleistung im Digitalisierungs-Umfeld als Asset verkaufen möchte. Die Frage ist immer, wie weit man dabei gehen möchte. Gewisse sehen den sicheren Aspekt eines vertrauenswürdigen Anbieters bei der Google Cloud an, bei anderen ist es vielleicht die AWS Cloud in Frankfurt, wo der Schlüssel bei AWS ist. Bei nochmals anderen ist es so, dass man selbst teilweise den Schlüssel hält. In diesen Fällen sind wir aber noch meilenweit von Trusted oder Confidential Cloud Computing Instanzen entfernt. Wir müssen einerseits unterscheiden, ob es um die sichere Kommunikation und Ablage geht, welche die Interaktion steigert, oder ob es um das Rechnen und ergebnisorientierte Datenbearbeiten an sich. In einer grundverschlüsselten Container-Umgebung kann man sehr vieles bewirken. Gewisse Geschäftsmodelle werden im Laufe der Zeit womöglich nicht mehr konkurrenzfähig sein ohne eine solche Lösung.

Frage: Welche Use Cases sehen Sie für den Einsatz von CC?

[2] Antwort: Wie man aggressive Datenbearbeitung in einer vertrauenswürdigen Art und Weise durchführen kann, finde ich eine spannende Frage. Der Klassiker ist, dass man sensitive Daten, welche hochgefährlich sind, wie bspw. aus dem Gesundheitsbereich, nur noch in solchen Bereichen durchführt. Im Gesundheitsbereich bestehen jedoch bereits gesetzlich sehr strenge Vorgaben, Zertifizierungsvorgaben und meistens darf kein anderer Bearbeitungszweck dahinterstecken.

[3] Viel spannender ist es aber bei Daten, welche an und für sich nicht so heikel wären, aber der Zweck heikel ist. Das ist zum Beispiel der Fall im Bereich der personalisierten Nutzung, welche in der Werbung für Konsumentengüter zu finden ist. Dann stellt sich die Frage, wie man mit grundbasierten Daten eine Zweckserweiterung in der Produktbewerbung herbeiführen kann. Mittels CC hat man die Datenbearbeitung nicht in einem personenbezogenen Aspekt durchgeführt, weil die Bearbeitung innerhalb der abgeschlossen Datenräume stattgefunden hat und der Zugriff technisch verunmöglicht

wurde. Gemäss dem neuen Urteil kann die theoretische Pseudonymisierung als Anonymisierung angeschaut werden. In diesem Bereich könnte man CC zukünftig nutzen. Das ist im Ergebnis nicht sehr nutzerfreundlich. Man führt eine Datenbearbeitung durch, welche betroffene Personen evtl. nicht wollen, aber man durch die Nutzung einer Technologie erlaubt ist. Klar kann man behaupten, dass die Bearbeitung durch die Nutzung der Technologie benutzerfreundlich geworden ist. Das ist ein anderes Thema. Dort sehe ich sehr spannende Entwicklungsmöglichkeiten.

Frage: Wie sieht es mit der Sekundärnutzung in der Forschung aus?

[4] Antwort: Den Personenbezug von Patientendaten hat man sowieso bereits entkoppelt und wenn nicht, schafft man Transparenz via das Einholen einer Bewilligung. Der Rest ist in den Grundlagen des Humanforschungsgesetzes geregelt. In diesem Bereich ist der Einsatz von CC evtl. vertrauensstiftend, sodass man mehr Möglichkeiten erhält, die Daten zu nutzen. Aber wie bereits erwähnt ist von Gesetzeswegen bereits sehr viele vorgegeben, meistens bereits bei der Einwilligungsbasis. Das schränkt die Möglichkeiten ein.

Frage: Wieso ist CC rechtlich gesehen von Nutzen?

[5] Antwort: Man muss berücksichtigen, dass es nicht für jede Datenbearbeitung CC benötigt. Es kommt immer auf die Konstellation an. CC eröffnet jedoch Optionen, insbesondere im Bereich der aggressiven Datenbearbeitung, wo ich Potenzial für die Nutzung zukünftig sehe. Ob es funktioniert, kann ich jedoch zum jetzigen Zeitpunkt nicht sagen.

Frage: Sind die Daten wirklich weniger sicher bei einem Cloud-Provider mit Standort in Europa, als wenn sie in der Schweiz sind, resp. woher kommen die vielen Vorbehalte zur Cloud?

[6] Antwort: Diese Überlegung kommt ganz klar von damals, als Cloud-Infrastrukturen noch sehr offene Umgebungen waren. Man hatte nicht einzelne Mandanten, resp. separate Container. Zudem wurde damals eine Speicherung (Cloud Storage) der Daten angeboten. Heute ist es ganz anders. Ob die Daten jetzt in Frankfurt auf der Azure Cloud weniger sicher sind, als wenn der Serverraum in Zürich ist, würde ich nicht sagen. Es sind einfach zwei unterschiedliche Aspekte. Im ersten Fall hat man rechtlich betrachtet eine Datenbekanntgabe ins Ausland und man muss die gesetzlichen Voraussetzungen erfüllen. Im zweiten Fall hat man das nicht. Aber auch diese Aussage ist nur bedingt korrekt.

In dem Moment, wo man bei einer amerikanisch betriebenen Cloud Implikationen aus FISA oder Cloud Act hat und der Zugriff aus den USA stattfindet, hat man ja auch eine Bekanntgabe, selbst wenn der Standort in Zürich ist. Jetzt ist nur noch offen, ob die US-Behörden wirklich zugreifen können. Das können sie nicht, wenn die Daten verschlüsselt sind. Dort kommt die Frage der Datensicherheit auf. Wenn man eine Vollverschlüsselung bieten kann und der Controller im Besitz des Schlüssels ist, dann können die Daten auch in die USA oder nach China ausgelagert werden. Aber das ist meistens nicht der Fall.

Frage: Kann man sich als Kunde nicht durchsetzen mit dem Argument, dass man sich im eigenen Land strafbar macht durch eine Datenherausgabe?

[7] Antwort: Das wird ja gebrochen mit den entsprechenden amerikanischen Gesetzen, welche das umgehen, sprich FISA oder der Cloud Act, welche den Zugriff verlangen. Das ist auch der Grund, dass diverse Behörden aus der Schweiz und auch Europa sagen, dass man gar keine Daten auf Cloud-Servern von amerikanischen Providern bearbeiten darf, unabhängig, an welchem Standort sich der Server befindet. Lösen kann man das einzig und allein über die Verschlüsselung, und dies nur, wenn du alleiniger Besitzer des Schlüssels bist. Die Provider haben die Wahl zwischen einem Gesetzesverstoss im eigenen Land, wo der Unternehmenssitz ist und die Steuern bezahlt werden, oder gegen einen Vertrag eines Kunden. Schlussendlich ist es eindeutig, für was der Provider sich entscheidet. Zusammengefasst kann man sagen, dass die Daten in einem Server in der Schweiz eines Schweizer Cloud-Providers sicherer sind, als wenn man die Daten in Frankfurt in einem AWS Server speichert, weil da im Hintergrund ein amerikanischen Unternehmen agiert. Wenn man jedoch eine Verschlüsselung hat, bei der ich der alleinige Eigentümer des Schlüssels bin, hat man technisch gesehen keine hohen Risiken. Aber man hat immer noch einen Datentransfer ins Ausland.

Fragen: Was halten Sie vom risikobasierten Ansatz?

[8] Antwort: Die Frage ist eher, wie risikoaffin ist man und wer trägt das Risiko. Bei einer rein rechtlichen Sicht insbesondere im Bereich der Datenumgebungen gibt es kein schwarz oder weiss. Man muss das Risiko dort ansetzen, wo man es noch kontrollieren kann. Nicht mehr kontrollieren kann ich es, wenn bspw. der Serverstandort für eine Public Staats-Cloud in China ist. Am Ende des Tages gibt es Behörden, welche sich klar gegen eine Migration in die Cloud äussern. Anstatt immer nur dagegen zu sprechen,

sollte man eher den Ansatz wählen, mitzuteilen, was man darf. Ich bin klar dafür, dass man nicht in schwarz und weiss denkt. Eine zu 100% sichere Lösung gibt es nicht.

Frage: Wie kann oder muss ein Controller die Integrität einer Technologie prüfen?

[9] Antwort: Das „prüfen müssen" entspricht der Einhaltung der Aufsichtspflichten gegenüber einem Anbieter. Da geht es um die Auftragsdatenbearbeitung. Dort hat man klare Vorgaben aus dem Gesetz. Der Krux liegt jedoch vielmehr in der Beurteilung. Viele können das nur unter Einbezug einer externen Beratung. Im besten Fall hat man eine IT-Abteilung, welche das beurteilen kann. Man muss bis zu einem gewissen Grad die Mindestpflichten einhalten, vertraglich sicher aufgestellt sein, bei Hochrisikogeschäfte, wo notwendig, Externe miteinbeziehen. Bei Standardgeschäften muss dafür gesorgt sein, dass alles sauber dokumentiert ist und ein Nachweis besteht, dass die Datenbearbeitung datenschutzkonform ist. Am Ende des Tages geht es darum, starke Argumente für eine Datenbearbeitung zu haben. Das hat aber noch nichts mit einem risikobasierten Ansatz zu tun. Wenn man keine Ahnung hat, was beschafft wird, sollte man die Finger davon lassen. In solchen komplexen Themen wie bei CC ist es aber allgemein sehr schwierig, den Durchblick zu haben. Das Ziel ist, die Grundidee verstanden zu haben und basierend darauf eine Beurteilung machen zu können.

Frage: Lösen sich die Bedenken der Cloud im Fall von CC auf, obwohl diese auch mit der Cloud verbunden ist?

[10] Antwort: Ich glaube das Problem lässt sich pragmatisch lösen. Das Problem hinsichtlich der Datenzugriffsrisiken und Datensicherheitsrisiken, welches man mit CC löst, löst man zirkularfaktisch somit auch bzgl. der Unsicherheit mit der Cloud. Man ist zwar auf der Cloud, aber es bringt einem nichts. Alles, was auf dieser Cloud passiert, ist so abgeschottet und mandatiert, dass kein Zugriff möglich ist. Irgendwo muss man die Bearbeitung ja laufen lassen. Man löst das Problem mit der Technologie.

Frage: Die Digitalisierung schreitet voran. Was muss passieren, damit Kundendaten auf einer Cloud im Ausland gelagert werden können, resp. wie wird das Vertrauen aufgebaut?

[11] Antwort: Ich glaube, wenn sich gewisse gesetzliche Regelungen ändern, so wie zum Beispiel beim Trans Atlantic Data Protection Framework, welches zurzeit ausgearbeitet wird, kann wieder mehr Vertrauen geschafft werden. Am Ende des Tages hilft nur

der Aspekt der Datensicherheit und nicht der rechtliche Aspekt. Ein Vertrag kann nicht automatisch die Datensicherheit und Vertrauen gewährleisten. Und in diesem Kontext ist der Datenverschlüsselungsaspekt wiederum zentral.

Frage: CC wechselt als technische Massnahme eine organisatorische Massnahme aus. Ist das die zukünftige Tendenz?

[12] Antwort: Jein. Ich glaube, dass diese Massnahmen immer parallel laufen. Es ist auch eine Frage der Struktur. Wer, wann, wo, wodurch und wieso zugreifen kann und welches Berechtigungskonzept ich habe sind Aspekte, welche es immer geben wird. Die technische Entwicklung wird jedoch zeigen, inwiefern CC bestehende Lösungen ersetzt.

Frage: Wo sehen Sie die grössten zukünftigen Herausforderungen in der Datenbearbeitung?

[13] Antwort: Einerseits sehe ich die voranschreitende digitale Globalisierung im Bereich Big Data als Herausforderung an. Dieser Bereich rutscht immer mehr in den Open-Data-Bereich hinein und die Grenzen verschwimmen ineinander. Das andere ist die automatisierte Einzelfallentscheidung.

Ende des Experteninterviews.