School of Management and Law

Zürcher Hochschule für angewandte Wissenschaften (ZHAW)

Bachelorarbeit

Verwendung von Cloud-Dienstleistungen mit Transfer(s) von Personendaten in Clouds von US-Anbietern/in die USA

Vorgelegt von:

Melanie Köpfli

BSc Wirtschaftsrecht

Matrikel-Nr.: 18678318

Betreut durch:

RA Marcel Griesinger

Abgabe:

18. Mai 2022

I. Management Summary

Der Transfer von personenbezogenen Daten in Clouds der USA regt immer wieder zur Diskussion an. Die zunehmenden regulatorischen Anforderungen bezüglich der Nutzung von US-Clouds, erschweren Unternehmen den Überblick über die einzuhaltenden Pflichten. Die vorliegende Arbeit soll die Hintergründe dieser Problematik aufzeigen und den Nutzern von Cloud Dienstleistungen aus den USA die aktuelle Situation in diesem Rechtsgebiet aufzeigen.

Um ein solides Basiswissen über die datenschutzrechtlichen Vorgaben zu erhalten, wird zuerst auf das Schweizer Datenschutzrecht und dessen Weiterentwicklung eingegangen. Da das Schweizer Recht in diesem Gebiet stark vom EU-Recht abhängig ist, wird auch auf diese Rechtsnormen eingegangen und wichtige Eckdaten dazu erläutert. Um den rechtlichen Rahmen dieser Arbeit abzurunden, wird anschliessend das amerikanische Recht insbesondere der US-Cloud Act analysiert.

Damit der Überblick möglichst umfassend ist, werden die aktuellen Entwicklungen der Datenübermittlung beobachtet und der Hintergrund des EU-US Verhältnis in Bezug auf den Datenschutz erläutert. Dabei liegt der Fokus besonders auf den Urteilen des EuGH, welche verschiedene Absprachen zwischen diesen zwei Parteien für ungültig erklärt hat. Mit dem Schrems I Urteil kippte das EuGH das Safe-Harbor Abkommen zwischen den USA und der EU. Auch das später entstandene Privacy Shield konnte die Sicherheitsbedenken des EuGH bei der Datenübermittlung nicht beseitigen. Durch die Ungültigkeit dieses Beschlusses mittels Schrems II Urteil, ist der Transfer von personenbezogenen Daten aus der EU in die USA nur noch über Standardvertragsklauseln möglich.

Auch für die Schweiz hatte das Schrems II Urteil einen grossen Einfluss. Die Standardvertragsklauseln der Schweiz sind jedoch stark an diese der EU angelehnt und in vielen Fällen werden diese übernommen. Im Jahre 2021 veröffentlichte die EU-Kommission neue Standardvertragsklauseln, welche wichtige Neuerungen beinhalten. So muss bei diesen neuen Standardvertragsklauseln jeweils das geeignete Modul für den Datenexporteur und -importeur ausgewählt werden und es sind zusätzliche Schutzmassnahmen zu ergreifen. Dabei sind die technischen und organisatorischen Massnahmen, welche zur Gewährleistung der Datensicherheit beitragen klar zu benennen.

Zusätzlich dazu müssen die Parteien Garantien sicherstellen, aufgrund welcher der Datenimporteur seinen Pflichten nachkommen kann, ohne dass er durch die Gesetze und Praktiken des Drittlandes daran gehindert wird. Diese Regelung ist von ausserordentlicher Bedeutung da durch die Parteien garantiert werden muss, dass die US-Behörden nicht auf die personenbezogenen Daten in der Cloud des Datenimporteurs zugreifen können.

Personendaten in US-Clouds zu übermitteln und gleichzeitig den Anforderungen der europäischen und Schweizer Datenschutzbestimmungen gerecht zu werden, erweist sich als schwierig. Die einfachste, jedoch unrealistischste Option zur Garantie der Datensicherheit ist der Verzicht der Nutzung von US-Clouds. Andere Möglichkeiten liegen in Auftragsverarbeiterverträgen mittels Standardvertragsklauseln oder internen Datentransfer-Folgenabschätzungen, wie sie anhand der dieser Arbeit vorliegenden Checkliste durchgeführt werden können.

Inhaltsverzeichnis

II. Literaturverzeichnis

BAUMGARTNER ULRICH/HANSCH GUIDO/ROTH HEIKO, Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten, ZD (2021) S. 608 ff.

BAZZI CLAUDIO, Internationale Wirtschaftsspionage, Eine Analyse des strafrechtlichen Abwehrdispositivs der Schweiz, Diss. Zürich, Zürich/Basel/Genf 2015.

BESSON SAMANTHA/BREITENMOSER STEPHAN/PETRIG ANNA/SASSÒLI MARCO/ZIEGLER ANDREAS R., Völkerrecht / Droit international public, Aide-Mémoire, 3. Aufl., Zürich/St. Gallen 2019.

BLECHTA GABOR P., Kommentar zu Art. 3 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

BRANDT JOCHEN, Datenschutz, in: Hauschka Christoph E./Moosmayer Klaus/Lösler Thomas (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., München 2016.

CONRAD ISABELL/SIARA CARSTEN, Endlich Lösungen für die konzerninterne Drittlandübermittlung von Beschäftigtendaten?, Neue Entwicklungen bei EU-Standardvertragsklauseln, EDSA-Empfehlungen und Art. 49 DS-GVO, ZD (2021) S. 471 ff.

EPINEY ASTRID, Allgemeine Grundsätze, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Bern 2011, S. 521 f.

ERNST STEFAN, Kommentar zu Art. 1 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

ERNST STEFAN, Kommentar zu Art. 2 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

ERNST STEFAN, Kommentar zu Art. 3 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

ERNST STEFAN, Kommentar zu Art. 4 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

GERMANN OSCAR ADOLF, Wirtschaftlicher Nachrichtendienst nach Art. 273 des schweizerischen Strafgesetzbuches, Wirtschaftspolitik und Wirtschaftsrecht mir Einschluss des Sozial- und Arbeitsrechtes 9 (1957) S. 12 ff.

HUSMANN MARKUS, Kommentar zu Art. 273 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch, Jugendstrafrecht, 4. Auflage, Basel 2019.

LANGE FILIP, Kommentar zu Art. 46 DSGVO, in: Brink Stefan/Wolff Heinrich Amadeus (Hrsg.), BeckOK Datenschutzrecht, 39. Edition, München 2022.

LIVSCHITZ MARK, Datenschutz in Compliance und Rechtsverfahren, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter, Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015.

MARTINI MARIO, Kommentar zu Art. 28 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundedatenschutzgesetz, 3. Aufl., München 2021.

MAURER-LAMBROU URS/KUNZ SIMON, Kommentar zu Art. 1 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

MAURER-LAMBROU URS/KUNZ SIMON, Kommentar zu Art. 2 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

MAURER-LAMBROU URS/STEINER ANDREA, Kommentar zu Art. 4 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

PAULY DANIEL A., Kommentar zu Art. 44 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

PAAL BORIS P./PAULY DANIEL A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021.

RAMPINI CORRADO, Kommentar zu Art. 13 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

ROSENTHAL DAVID, Kommentar zu Art. 273 StGB, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008.

ROSENTHAL DAVID, Microsoft Cloud für Schweizer Anwälte, Anwaltsrevue: Das Praxismagazin des schweizerischen Anwaltsverbandes (2021) S. 443 ff.

SIDLER IRIS/VASELLA DAVID, Aus Safe Harbor wird Privacy Shield: Folgen des Urteils des EuGH i.S. Schrems, Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht (2016), S. 185-195.

SCHMITZ BARBARA/SPIES AXEL, DSK: US-Gutachten zur Risikoeinschätzung bei Datentransfers (DTIA) veröffentlicht, (https://rsw.beck.de/cms/?toc=ZD.root&docid=445340), besucht am: 30. April 2022.

STRASSEMEYER LAURENZ/SCHEFZIG JENS/FLEMMING MOOS, in: Moos Flemming/Schefzig Jens/Marian Alexander Arning (Hrsg.), Praxishandbuch DSGVO einschliesslich BDSG und spezifischer Anwendungsfälle, 2. Aufl., Frankfurt 2021.

THÜSING GREGOR/FORST GERRIT, Internationale Datenübermittlung, in: Thüsing Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance, Effektive Compliance im Spannungsfeld von DS-GVO, BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 3. Aufl., München 2021.

TRECHSEL STEFAN/VEST HANS, Kommentar zu Art. 273 StGB, in: Trechsel Stefan/Pieth Mark (Hrsg.), Praxiskommentar Schweizerisches Strafgesetzbuch, 4. Aufl., Zürich 2021.

VASELLA DAVID, Microsoft ist nicht verpflichtet, der US-Regierung ausserhalb der USA liegende Nutzerdaten herauszugeben, Beitrag vom 14. Juli 2016, (https://datenrecht.ch/microsoft-ist-nicht-verpflichtet-der-us-regierung-ausserhalb-der-usa-liegende-daten-herauszugeben/), besucht am 16. März 2022.

WEBER ROLF H., Datenexport in die USA – neue Welt nach Schrems II?, Zeitschrift für Europarecht (2021) S. 24 ff.

WEBER ROLF H., E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich 2010.

WEBER ROLF H./HENSELER SIMON, Daten-Governance und Cloud Banking im neuen Datenschutzrechtsumfeld, Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (2020) S. 604 ff.

WIDMER BARBARA, Safe-Harbor – wenn weniger nicht genügt, Zeitschrift für Datenrecht und Informationssicherheit (2015) S. 146 ff.

III. Materialienverzeichnis

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413 ff.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff.

Bundesamt für Justiz, Normkonzept zur Revision des Datenschutzgesetzes, Bericht der Begleitgruppe Revision DSG vom 29. Oktober 2014, (https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf.download.pdf/ber-normkonzept-d.pdf) besucht am: 15. April 2022.

Commission implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, (https://ec.europa.eu/info/law/law-topic/data-protection_en), besucht am: 18. April 2022.

Draft of Commission implementing Decision of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Datenschutz-Standardvertragsklauseln-fur-die-Ubermittlung-personenbezogener-Daten-in-Nicht-EU-Lander-Durchfuhrungsrechtsakt-_de), besucht am: 5. Mai 2022.

IV. Sonstige Materialien

Brief des US Secretary of State John Kerry an Kommissarin Vˇera Jourová vom 22. Februar 2016, (https://www.ftc.gov/system/files/attachments/eu-us-privacy-shield-framework/eu_us_privacy_shield_full_textpdf.pdf), besucht am: 18. April 2022.

Brief des Director of National Intelligence an das US Department of Commerce und die US International Trade Administration vom 22. Februar 2016, (https://www.ftc.gov/system/files/attachments/eu-us-privacy-shield-framework/eu_us_privacy_shield_full_textpdf.pdf), besucht am: 18. April 2022.

Briefwechsel vom 1. und 9. Dezember 2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika, SR 0.235.233.6.

Bundesamt für Justiz, Bericht vom 17. September 2021 zum US CLOUD Act, (https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html), besucht am: 25. März 2022.

Bundesamt für Justiz, Stärkung des Datenschutzes, (https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html), besucht am: 20. April 2022.

Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien vom März 2019, (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf), besucht am: 17. April 2022.

Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden für Anbieter: innen von Telemedien vom 20. Dezember 2021, (https://datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf), besucht am 17. April 2022.

Datenschutzkonferenz, Pressemitteilung Datenschutz-Aufsichtsbehörden: Ergänzende Prüfungen und Maßnahmen trotz neuer EU-Standardvertragsklauseln für Datenexporte nötig vom 21. Juni 2021, (https://www.datenschutz.de/wp-content/uploads/kalins-pdf/singles/datenschutz-aufsichtsbehoerden-ergaenzende-pruefungen-und-massnahmen-trotz-neuer-eu-standardvertragsklauseln-fuer-datenexporte-noetig.pdf), besucht am: 24. April 2022.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge vom 27. August 2021, (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html), besucht am 27. April 2022.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Staatenliste vom 15. November 2021, (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/20211115_Länderliste_d.pdf.download.pdf/20211115_Länderliste_d.pdf), besucht am: 30. April 2022.

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 vom 8. September 2020, (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html), besucht am: 21. April 2022.

CNIL, Utilisation de Google Analytics et transferts de données vers les États-Unis: la CNIL met en demeure un gestionnaire de site web vom 10. Februar 2022, (https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure), besucht am: 20. April 2022.

Mitteilung der Kommission zur Transatlantic Data Flows: Restoring Trust through Strong Safeguards, vom 29. Februar 2016, (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0117&from=EN), besucht am 1. April 2022.

Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/52/EG.

European Data Protection Board EDPB, Empfehlungen 01/2020 zu Massnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 18. Juni 2021, (https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf), besucht am: 2. Mai 2022.

European Data Protection Board EDPB, Stellungnahme 23/2018 zu den Vorschlägen der Kommission über Europäische Herausgabe- und Sicherheitsanordnungen für elektronische Beweismittel in Strafsachen (Artikel 70 Absatz 1 Buchstabe b) vom 26. September 2018, (https://edpb.europa.eu/sites/default/files/files/file1/edpb-2018-09-26-eevidence_de.pdf), besucht am: 2. Mai 2022.

European Data Protection Supervisor EDPS, Stellungnahme 2/2019 zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln vom 2. April 2019, (https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_eu_us_agreement_e-evidence_en_de.pdf), besucht am: 30. April 2022.

European Data Protection Supervisor EDPS/European Data Protection Board EDPB, Annex. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence vom 10. Juli 2019, (https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf) besucht am: 30. März 2022.

Medienmitteilung zum EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield vom 2. Februar 2016, (https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216) besucht am: 29. März 2022.

Bundesrat, Medienmitteilung zu Revision der Datenschutzverordnung: Bundesrat eröffnet Vernehmlassung vom 23. Juni 2021, (https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html), besucht am 20. April 2022.

Eidgenössischen Justiz- und Polizeidepartement (EJPD), Medienmitteilung zu Den Datenschutz stärken vom 9. Dezember 2011, (https://www.bj.admin.ch/ejpd/de/home/aktuell/news/2011/2011-12-09.html), besucht am: 20. April 2022.

Eidgenössischen Justiz- und Polizeidepartement (EJPD), Medienmitteilung zu Der Datenschutz soll gestärkt werden vom 1. April 2015, (https://www.bj.admin.ch/ejpd/de/home/aktuell/news/2015/2015-04-010.html), besucht am: 20. April 2022.

Eidgenössischen Justiz- und Polizeidepartement (EJPD), Medienmitteilung zu Mehr Transparenz und stärkere Kontrolle über die eigenen Daten vom 21. Dezember 2016, (https://www.bj.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html), besucht am: 20. April 2022.

Eidgenössischen Justiz- und Polizeidepartement (EJPD), Medienmitteilung zu Den Datenschutz verbessern und den Wirtschaftsstandort stärken vom 15. September 2017, (https://www.bj.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html), besucht am: 20. April 2022.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Mitteilung zu Swiss-US Privacy Shield: neuer Rahmen für die Datenübermittlungen in die USA vom 11. Januar 2017, (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa/swiss-us-privacy-shield--neuer-rahmen-fuer-datenuebermittlungen-.html), besucht am 6. April 2022.

Europäische Kommission, Memo zur Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA – Häufig gestellte Fragen vom 27. November 2013, Memo/13/1059, (https://ec.europa.eu/commission/presscorner/detail/de/MEMO_13_1059), besucht am: 4. April 2022.

Nationalversammlung Frankreich, Bericht vom 26. Juni 2019 zu Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale, (https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf), besucht am: 23. März 2022.

U.S. Department of Commerce, Annex II, EU-U.S. Privacy Shield Framework Principles vom 23. Februar 2016, (https://www.ftc.gov/system/files/attachments/eu-us-privacy-shield-framework/eu_us_privacy_shield_full_textpdf.pdf), besucht am: 18. April 2022.

U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act, White Paper vom April 2019, (https://www.justice.gov/dag/page/file/1153436/download), besucht am: 30. März 2022.

V. Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt
BeckOK	Beck'sche Online-Kommentare
BJ	Bundesamt für Justiz
BJM	Basler juristische Mitteilungen
BL	Basel-Landschaft
BSc	Bachelor of Science
BSK	Basler Kommentar
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BYOK	bring your own key
BYOE	bring your own encryption
CNIL	Commission Nationale de l'Informatique et des Libertés
CSP	Anbieter von Kommunikationsdiensten
Diss.	Dissertation
DOJ	U.S. Department of Justice
DSB	Datenschutzbehörde Österreich
DSG	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1

DSGVO	Verordnung 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)
DSK	Datenschutzkonferenz
DTIA	Datentransfers
E.	Erwägung
EJPD	Eidgenössische Justiz- und Polizeidepartement
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDSA	Europäischer Datenschutzausschluss
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) vom 4. November 1950, SR 0.101
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
f.	folgende
ff.	fortfolgende
FISA 702	50 U.S. Code § 1881, United States Code, 2006 Edition, Supplement 5, Title 50 - war and national defense
FTC	Free Trade Commission
GRCh	Charta der Grundrechte der Europäischen Union, C 326/395 vom 26.10.2012

ggü.	gegenüber
GZ	Geschäftszahl
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
i.S.	im Sinne
i.S.v.	im Sinne von
lit.	litera
LLC	Limited Liability Company
nDSG	neues Bundesgesetz über den Datenschutz tritt gemäss Art. 74 nDSG mittels Bundesbeschluss in Kraft
NGO	Nichtregierungsorganisation
Nr.	Nummer
NSA	National Security Agency
OGer BL	Obergericht Basel-Landschaft
PK	Praxiskommentar
RA	Rechtsanwalt
Rs.	Rechtssache
Rz.	Randziffer
S.	Seite
SCA	Stored Communications Act, 18 U.S. Code Chapter 121 - stored wire and electronic communications and transactional records access
SCC	Standardvertragsklauseln
SR	Systematische Rechtssammlung

StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
StIGH	Ständiger Internationaler Gerichtshof
UNO	Vereinigte Nationen
UNO Charta	Charta der Vereinigten Nationen vom 26. Juni 1945, SR 0.120
US	Vereinigte Staaten
USA	Vereinigte Staaten von Amerika
US Cloud Act	Clarifying Lawful Overseas Use of Data Act, A bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes
usw.	und so weiter
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993, SR 235.11
Vgl.	vergleiche
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZGB	Schweizerisches Zivilgesetzbuch (ZGB) vom 10. Dezember 1907, SR 210

1 Einleitung

Im Rahmen der Globalisierung und des technischen Fortschritts werden laufend mehr personenbezogene Daten in die USA übermittelt, besonders mittels Cloud-Computing. Diese Arbeit soll einen Überblick verschaffen, wie sich der Transfer von personenbezogenen Daten in die USA während den letzten Jahren verändert hat und inwiefern diese Übermittlungen zulässig sind.

Bei Cloud-Computing, kurz Clouds, können Unternehmen Rechnerkapazitäten über das Internet nutzen, welche von Dritten angeboten werden. Über das Internet werden diverse Rechnerleistungen von unterschiedlichen Standorten abgerufen. Es handelt sich dabei um Speicherplatznutzung oder auch um ganze IT-Infrastrukturen.[1]

In einem ersten Schritt wurde in der vorliegenden Arbeit auf die rechtlichen Rahmenbedingungen des Schweizer Datenschutzrechts und dem europäischen eingegangen. Unter anderem wurde das amerikanische Recht in Form des US-Cloud Acts analysiert. In einem nächsten Schritt wurde der Fokus auf die Entwicklung des datenschutzrechtlichen Verhältnisses zwischen den USA und der EU gelegt, um zu ergründen, weshalb der Datentransfer in die USA ein heikles und aktuelles Thema ist. In diesem Zusammenhang wurde das Instrument erläutert, mit welchem der Datentransfer in die USA zulässig sein soll und dessen anspruchsvolle Umsetzung.

Grundsätzlich legt die vorliegende Arbeit den Fokus auf die Übermittlung der Daten in die USA. Ungeachtet dessen wird der Vollständigkeit halber nicht immer gezielt die USA angesprochen. Da das Schweizer Datenschutzrecht stark abhängig von diesem der EU ist, wurde wenn immer möglich und sinnvoll auf beide Gesetzgebungen Rücksicht genommen. Hinsichtlich der Methodik werden die der Gesetzgebung entsprechenden Kommentare sowie Sekundärliteratur berücksichtigt.

Neben der theoretischen Klärung der Fragestellung soll eine Checkliste in kompakter und anschaulicher Form aufzeigen, wie Unternehmen gewährleisten können, dass der Transfer von Personendaten in die USA über ihren US-Cloudanbieter den Vorgaben der EU entspricht. Diese Thematik geniesst unter anderem aufgrund der neuen Vorgaben der EU, und folglich der Schweiz, einen hohen Praxisbezug und ist überaus aktuell.

---

[1] BRANDT, Rz. 144.

2 Rechtliche Rahmenbedingungen

2.1 DSG

Das Datenschutzgesetz (DSG)[2] trat in der Schweiz per 1. Juli 1993 in Kraft und wurde zur Schliessung der Lücken des Persönlichkeitsschutzes nach Art. 28 ff. ZGB[3] im Hinblick auf die Datenbearbeitungen geschaffen. Der Gesetzgeber empfand die Kriterien der Zulässigkeit der Datenbearbeitung als zu unpräzise. Das DSG hat privatrechtliche Wirkungen wie auch öffentlich-rechtliche, basierend auf dem damals ungeschriebenen Grundrecht der persönlichen Freiheit und Art. 8 EMRK[4] über das Recht auf Achtung des Privat- und Familienlebens.[5] In der Zwischenzeit ist der Datenschutz auch auf Verfassungsebene festgeschrieben. Einerseits durch die persönliche Freiheit aus Art. 10 Abs. 2 BV[6], andererseits auch mittels Schutzes der Privatsphäre im Sinne von Art. 13 BV.[7]

Der Zweck des Datenschutzgesetzes wird nach Art. 1 DSG bestimmt und umfasst «den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden». Hier zeigt sich die zweiteilige Wirkung des DSG in dem sich der Schutz der Persönlichkeit auf den Austausch von Informationen zwischen Privaten bezieht und der Schutz der Grundrechte primär auf den Schutz vor staatlichen Behörden abzielt.[8] Die Persönlichkeit soll im weiteren Sinn verstanden werden und umfasst alle physischen, psychischen, moralischen und sozialen Werte, die einer Person aufgrund ihrer Existenz gebühren.[9] Das DSG möchte nicht nur erfolgte Verletzungen sanktionieren, sondern auch präventiv agieren und bevorstehende oder potenzielle Verletzungen verhindern. Jede Bearbeitung oder Aufbewahrung von Daten hat Potential für eine Persönlichkeitsverletzung. Die Bearbeitung von Personendaten kann jedoch auch erfolgen, ohne dass es eine Verletzung der Persönlichkeit zur Folge hat.[10]

---

2 Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1.
3 Schweizerisches Zivilgesetzbuch (ZGB) vom 10. Dezember 1907, SR 210.
4 Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) vom 4. November 1950, SR 0.101.
5 MAURER-LAMBROU/KUNZ, BSK, Rz. 4 zu Art. 1 DSG.
6 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.
7 MAURER-LAMBROU/KUNZ, BSK, Rz. 5 zu Art. 1 DSG.
8 MAURER-LAMBROU/KUNZ, BSK, Rz. 6 zu Art. 1 DSG.
9 BBl 1988, S. 418.
10 MAURER-LAMBROU/KUNZ, BSK, Rz. 12 zu Art. 1 DSG.

2.1.1 Entwicklungsgeschichte nDSG

Das neue Datenschutzgesetz (nDSG)[11] soll ab dem 1. September 2023 in Kraft gesetzt werden. Der Gesetzesentwurf zur Totalrevision verfolgt das Ziel der Stärkung des Datenschutzes, indem die Datenbearbeitung transparenter sein soll, sowie die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten optimiert werden sollen. Die Schwächen des DSG aufgrund der rapiden technologischen Entwicklungen, sollen behoben werden. Zudem sollen die Bearbeitungsverantwortlichen in ihrem Verantwortungsbewusstsein gestärkt werden, da sie bereits bei der Planung neuer Datenbearbeitungen Datenschutzvorschriften einhalten müssen. Letztendlich soll durch die Revision die Wettbewerbsfähigkeit der Schweiz, mittels vereinfachter Datenbekanntgabe ins Ausland, optimiert und die Digitalisierung gefördert werden. Insbesondere soll die Revision die Entwicklung des EU-Datenschutzrechts berücksichtigen. Damit soll es der Schweiz möglich gemacht werden, die Schengen-relevante EU-Richtlinie der Datenschutz-Grundverordnung (DSGVO)[12] umzusetzen. Die Revision des DSG war immer wieder Thema in diversen parlamentarischen Vorstössen, dies zeigt den politischen Willen dieser Revision.[13]

Am 9. Dezember 2011 beauftrage der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD) gesetzgeberische Schritte zur Stärkung des Datenschutzes zu prüfen. Der Bundesrat wollte aufgrund der rasanten, technologischen und gesellschaftlichen Entwicklungen im Bereich der Datenerhebung, -verknüpfung, -weitergabe und -auswertung, die Entwicklungen in der EU evaluieren und prüfen ob und in welcher Form das DSG anzupassen ist.[14] Das EJPD sollte dem Bundesrat bis Ende 2014 Vorgehensvorschläge unterbreiten. Die Zuständigkeit dazu lag beim Bundesamt für Justiz (BJ), welches vom September 2012 bis Oktober 2014 eine Arbeitsgruppe eingesetzt hatte, um den Handlungsbedarf abzuschätzen. Ihre Erkenntnisse fassten sie in einem Bericht zusammen, welcher dem Bundesrat zur Kenntnisnahme übergeben wurde.[15] Basierend auf diesem Bericht, gab der Bundesrat dem EJPD den Auftrag einen Vorentwurf für die Revision des DSG auszuarbeiten. Unter Berücksichtigung der laufenden Entwicklungen in der EU

---

11 neues Bundesgesetz über den Datenschutz tritt gemäss Art. 74 nDSG mittels Bundesbeschluss in Kraft.

12 Verordnung 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).

13 BBl 2017, S. 6943 f.

14 EJPD, Medienmitteilung, 2011.

15 BJ, Normkonzept, S. 3 f.

soll der Vorentwurf bis spätestens Ende August 2016 unterbreitet werden.[16] Der Bundesrat schickte den Vorentwurf im Dezember 2016 in die Vernehmlassung[17] und verabschiedete am 15. September 2017 die Botschaft zur Totalrevision des DSG.[18]

Während der Herbstsession 2020 hat das Parlament das nDSG verabschiedet. Durch die Totalrevision sollen die persönlichen Daten besser geschützt werden, indem der Datenschutz am technologischen Stand angepasst wurde, die Selbstbestimmung gefördert sowie die Transparenz gestärkt wird. Diverse Bestimmungen des nDSG müssen auf Verordnungsebene präzisiert werden, bevor das nDSG in Kraft treten kann. Das Vernehmlassungsverfahren dauerte bis am 14. Oktober 2021, die Verordnung soll dann mit dem nDSG zusammen in Kraft treten.[19] Das BJ informierte im März 2022 darüber, dass das nDSG ab 1. September 2023 in Kraft treten soll, der formelle Entscheid des Bundesrats steht jedoch noch aus.[20]

2.1.2 Anwendungsbereich

Die weiteren Ausführungen über das DSG basieren auf dem heutigen Stand des Rechts[21]. Der Geltungsbereich des DSG wird in Art. 2 Abs. 1 DSG geregelt. Es gilt für private Personen wie auch Bundesorgane, welche Daten natürlicher und/oder juristischer Personen bearbeiten.[22] Das DSG ist anwendbar für das «Bearbeiten von Daten», darunter versteht man gemäss Art. 3 lit. e DSG «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten». Es wird nicht zwischen manueller und automatisierter Datenbearbeitung unterschieden und jede Form der Datenbearbeitung wird vom DSG erfasst.[23]

Es bestehen keine Bestimmungen im DSG bezüglich des räumlichen Geltungsbereichs. Aufgrund des Territorialitätsprinzips kommen die öffentlich-rechtlichen Vorschriften des DSG nur für Ereignisse in der Schweiz zur Anwendung, dabei muss der Ort der Personendatenbearbeitung in der Schweiz sein. Es fallen jedoch auch Sachverhalte die

16 EJPD, Medienmitteilung, 2015.
17 EJPD, Medienmitteilung, 2016.
18 EJPD, Medienmitteilung, 2017.
19 Bundesrat, Medienmitteilung.
20 BJ, Stärkung des Datenschutzes.
21 Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1, Stand am 1. März 2019.
22 MAURER-LAMBROU/KUNZ, BSK, Rz. 2 zu Art. 2 DSG.
23 MAURER-LAMBROU/KUNZ, BSK, Rz. 3 zu Art. 2 DSG.

Auswirkungen auf die Schweiz haben unter den Anwendungsbereich des DSG.[24] Dies kann der Fall sein, wenn beispielsweise Internetseiten in der Schweiz abgerufen werden, diese jedoch im Ausland publiziert wurden.[25]

In Art. 2 Abs. 2 DSG sind Bereiche aufgeführt, auf welche das DSG keine Anwendung findet. «Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt» sind gemäss lit. a nicht im Geltungsbereich des DSG.[26] Damit ist die Verwendung von Personendaten im engeren Privat- und Familienleben zu verstehen.[27] Das DSG ist ebenso nicht anwendbar auf Beratungen der Bundesversammlung und der parlamentarischen Kommission, auf hängige Zivilprozess-, Straf-, internationale Rechtshilfe- sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme des erstinstanzlichen Verwaltungsverfahren, auf öffentliche Register des Privatrechtverkehrs und Personendaten, welche vom Internationalen Komitee vom Roten Kreuz bearbeitet werden.[28]

2.1.3 Personendaten

Das DSG schützt die Bearbeitung von Personendaten natürlicher und juristischer Personen. Sachdaten, Daten welche nicht als Personendaten qualifizierbar sind, werden nicht vom DSG erfasst.[29] Gemäss Art. 3 lit a. DSG sind Personendaten «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Mit «alle Angaben» sind jegliche Informationen zu verstehen, welche auf die Vermittlung, den Empfang oder auf die Aufbewahrung gerichtet sind, obgleich es sich um subjektive Angaben, wie Meinungen, oder objektive Angaben, wie bestimmte physische Merkmale, handelt. Ausserdem ist es unwesentlich, wie eine Angabe erfolgt, sei es als Zeichen, Wort, Bild, Ton oder einer Kombination dieser. Ebenfalls unwesentlich ist die Art des Datenträgers, auf welchem die Informationen gespeichert sind.[30] Als Personendaten sind alle Angaben zu qualifizieren die sich einer oder mehrere natürlichen oder juristischen Personen zuordnen lassen.[31]

Die Angaben müssen sich auf eine bestimmte oder bestimmbare Person beziehen bzw. beziehen können. Die Information muss also lediglich mit einer natürlichen oder

---

[24] MAURER-LAMBROU/KUNZ, BSK, Rz. 19b zu Art. 2 DSG.
[25] Urteil des Bundesverwaltungsgerichts, A-7040/2009 vom 30. März 2011, E. 5.4.2.
[26] MAURER-LAMBROU/KUNZ, BSK, Rz. 20 f. zu Art. 2 DSG.
[27] BBl 1988, S. 441.
[28] MAURER-LAMBROU/KUNZ, BSK, Rz. 23 ff. zu Art. 2 DSG.
[29] BLECHTA, BSK, Rz. 3 zu Art. 3 DSG.
[30] BLECHTA, BSK, Rz. 6 zu Art. 3 DSG.
[31] BBl 1988, S. 444.

juristischen Person in Verbindung gebracht werden können.[32] Eine Person ist bestimmt, sofern sich aus den Angaben ergibt, dass sie sich ausschliesslich auf diese konkrete Person beziehen. Bestimmbar ist eine Person, wenn sie anhand der Daten nicht eindeutig identifiziert werden kann, es jedoch aufgrund des Kontexts der Informationen möglich ist, deren Identität festzustellen.[33] Wie der Bezug zur betroffenen Person hergestellt wird, ist nicht relevant. Der Aufwand zur Identifizierung darf jedoch nicht übermässig sein, sonst ist die Person nicht mehr bestimmbar. Es ist anhand objektiver Kriterien zu beurteilen, ob Bestimmbarkeit vorliegt, dabei ist auch der Stand der Technik und die technische Entwicklungsmöglichkeit während der Datenbearbeitung zu beachten. Die Pseudenomysierung von Personendaten hat eine Verschleierung der Identität der betroffenen Person zu Folge. Pseudonomyisierte Daten sind so weit als Personendaten zu qualifizieren, wie sie wieder identifiziert werden können. Anonyme Daten hingegen sind keine Personendaten. Die Daten, welche sich zuvor auf eine bestimmte oder bestimmbare Person bezogen haben, sind irreversibel anonymisiert worden. Aufgrund der heutigen Technik ist es äussert selten, dass Daten nicht reidentifiziert werden können und demnach anonym sind.[34]

2.1.4 Bearbeitungsgrundsätze

Art. 4 DSG beinhaltet als Grundsatzartikel die wesentlichsten materiellen Grundsätze, die eingehalten werden müssen, wenn Personendaten bearbeitet werden. Hiermit soll vermieden werden, dass Daten exzessiv, uneingeschränkt oder zweckentfremdet bearbeitet werden.[35] Personendaten dürfen gemäss Art. 4 Abs. 1 DSG nur rechtmässig bearbeitet werden. Damit die Bearbeitung rechtmässig ist, muss sie nach Treu und Glauben erfolgen und verhältnismässig sein.[36] Der Grundsatz von Treu und Glauben wird ausdrücklich in Art. 2 Abs. 1 ZGB erwähnt und gilt in allen Bereichen des Rechts als fundamentale Norm. Es gebietet ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr. Auch in der Bundesverfassung ist dieses Prinzip in Art. 9 explizit erwähnt und Art. 5 Abs. 3 BV bindet staatliche Organe und Private an das Handeln nach Treu und Glauben. Dieses Handeln muss für jede Bearbeitung von Personendaten angewendet werden. Die Verhältnismässigkeit in der Datenbearbeitung ergibt sich aus Art. 5 Abs. 2 BV. Das Verhältnismässigkeitsprinzip wird eingehalten, wenn die Massnahme geeignet ist das verfolgte Ziel zu

---

[32] BLECHTA, BSK, Rz. 7 zu Art. 3 DSG.
[33] BBl 1988, S. 444.
[34] BLECHTA, BSK, Rz. 10 ff. zu Art. 3 DSG.
[35] MAURER-LAMBROU/STEINER, BSK, Rz. 2 zu Art. 4 DSG.
[36] WEBER, E-Commerce und Recht, S. 448.

erreichen, erforderlich, also der geringstmögliche Eingriff um die privaten Interessen zu wahren und zumutbar ist.[37] Der Datenbearbeiter darf folglich nur Daten erheben und bearbeiten, die für einen bestimmten Zweck geeignet sind und welche er objektiv tatsächlich benötigt. Es muss ein adäquates Verhältnis zwischen dem Bearbeitungszweck und der damit verbundenen Persönlichkeitsbeeinträchtigung bestehen. Werden mehr Daten erhoben und weiterverarbeitet, als nach dem Zweck notwendig sind, so ist das Verhältnismässigkeitsprinzip verletzt.[38] Ob dies der Fall ist, hängt vom verfolgten Zweck und den existierenden Vertragsbeziehungen ab, folglich dem Gesamtkontext.[39]

Der Zweck, welcher bei der Beschaffung von Personendaten angegeben worden ist oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist, gilt als Zweck der Personendatenbearbeitung. Die betroffenen Personen sollen wissen, aus welchem Grund ihre Daten bearbeitet werden.[40] Durch den heutigen Stand der Technik ist die Wahrscheinlichkeit, dass Daten für andere Zwecke als für den ursprünglichen bearbeitet werden, stark angestiegen. Dies insbesondere auch aufgrund der Verfügbarkeit enormer Datenmengen.[41] Daten, welche nicht mehr benötigt werden, sind zu löschen.[42]

Gemäss Art. 4 Abs. 4 DSG muss es für die betroffene Person erkennbar sein, ob und wann die sie betreffenden Daten beschafft werden und zu welchem Zweck. Gemäss dem Wortlaut dieser Norm muss aber nur das Beschaffen erkennbar sein, nicht die Weiterbearbeitung der Daten. Erkennbarkeit in diesem Sinne bedeutet, dass eine betroffene Person aus den gegebenen Umständen mit der Beschaffung von Daten und dem Zweck der Bearbeitung rechnen musste oder sie angebracht aufgeklärt wurde. Je erheblicher die Datenbearbeitung ist, desto höhere Anforderungen werden an die Transparenz gestellt.[43] Absatz 5 von Art. 4 DSG erfordert für die Datenbearbeitung eine Einwilligung der betroffenen Person und gibt die Voraussetzungen zu deren Gültigkeit an.[44] Der Betroffene muss über alle notwendigen Informationen wie die Art und den Umfang der Datenbearbeitung, den Datenbearbeiter, Zweck der Datenbearbeitung und allfällige Risiken verfügen.[45]

---

37 MAURER-LAMBROU/STEINER, BSK, Rz. 7 f. zu Art. 4 DSG.
38 BBl 1988, S. 450.
39 WEBER, E-Commerce und Recht, S. 450.
40 BBl 1988, S. 451.
41 MAURER-LAMBROU/STEINER, BSK, Rz. 13 zu Art. 4 DSG.
42 WEBER, E-Commerce und Recht, S. 452.
43 MAURER-LAMBROU/STEINER, BSK, Rz. 16a ff. zu Art. 4 DSG.
44 MAURER-LAMBROU/STEINER, BSK, Rz. 16f zu Art. 4 DSG.
45 EPINEY, Rz, 17.

2.2 DSGVO

Die DSGVO bildet das Fundament des europäischen Datenschutzrechts. Die seit dem 25. Mai 2018 geltende DSGVO gilt als Grundpfeiler für datenschutzrechtliche Diskussionen auf europäischer Ebene sowie auf nationaler Ebene in den Mitgliedsstaaten der europäischen Union.[46] Das Ziel der DSGVO war die Vollharmonisierung des Datenschutzrechts im EU-Raum. Nationale Datenschutzgesetze mussten deshalb angepasst werden, jedoch bestehen diese weiterhin, da die DSGVO einige Ausnahmevorschriften zugunsten des nationalen Rechts vorsieht.[47] Die DSGVO stiess bereits früh auf Kritik von verschiedenen Seiten und zieht auch heute noch Kritik auf sich. Sie wird je nach Auffassung als entweder zu weitegehend oder nicht ausreichend beurteilt.[48] Der Zweck der DSGVO wird nach Art. 1 DSGVO bestimmt und betrifft die datenschutzrechtlichen Grundrechte und Grundfreiheiten natürlicher Personen. Wie auch den Verweis, dass dieser Schutz den freien Datenverkehr in der EU nicht einschränken darf oder gar verbieten. Die personenbezogenen Daten von natürlichen Personen sollen gemäss Erwägungsgrund 10 der DSGVO in der gesamten EU gleichmässig und übereinstimmend angewandt werden.[49]

Das Recht auf Schutz von personenbezogenen Daten ist gemäss Art. 1 Abs. 2 DSGVO ein Grundrecht und die DSGVO dient explizit dem Schutz ebendieses Grundrechts.[50] Der Schutz von personenbezogenen Daten ist kein Bürgerrecht, sondern ein Menschenrecht. Die DSGVO gewährt gemäss Erwägungsgrund 14 ihren Schutz allen natürlichen Personen, deren personenbezogene Daten verarbeitet werden, ungeachtet der Staatsangehörigkeit oder des Aufenthaltsortes. Er richtet sich an den Staat sowie auch gegen private Datenverarbeiter. Die DSGVO soll nach Erwägungsgrund 2 «zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen» beitragen. Sie soll aber gemäss Erwägungsgrund 4 auch «im Dienst der Menschheit stehen». Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht

[46] PAAL/PAULY, Rz. 1.
[47] PAAL/PAULY, Rz. 2.
[48] PAAL/PAULY, Rz. 7.
[49] ERNST, Rz. 1 zu Art. 1 DSGVO.
[50] ERNST, Rz. 2 zu Art. 1 DSGVO.

und muss deshalb mittels Verhältnismässigkeitsprinzip gegen andere Grundrechte abgewogen werden.[51]

2.2.1 Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich ergibt sich aus Art. 2 DSGVO und besagt, dass die DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, wie auch für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, gilt. Adressaten sind öffentliche sowie nicht öffentliche Stellen.[52] Gemäss Art. 4 Nr. 2 DSGVO ist die Verarbeitung jeder «mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung». Der Begriff des automatisierten Verfahrens ist sehr weitläufig und schliesst im Grunde genommen jede Form der Datenverarbeitungsanlagen ein. Auch Computer jeder Grösse, Smartphones, Überwachungsanlagen, etc., sind erfasst. Sind personenbezogene Daten in der Nutzung von Computer, Internet, usw. beinhaltet, so führt dies zur Anwendbarkeit der DSGVO.

Die automatisierte und teilweise automatisierte Datenverarbeitung unterscheidet sich durch die Erhebung mit und ohne händische Zwischenschritte. Teilweise automatisierte Verarbeitung liegt vor, wenn ein Mensch die Daten in ein System eintippt, hingegen geschieht die automatisierte Datenverarbeitung mittels gesteuerten Verfahrens selbstständig und resultiert in einer programmgesteuerten Zugänglichkeit und Auswertung der Daten. Nicht automatisierte Verarbeitung bezieht sich auf den analogen Bereich der Verarbeitung.[53] Sobald personenbezogene Daten in einem Dateisystem abgespeichert sind, fallen sie unter den sachlichen Anwendungsbereich der DSGVO. Sie unterstehen ihm auch, wenn die Daten in Zukunft in einem Dateisystem gespeichert werden sollen und gespeichert werden könnten.[54]

---

[51] ERNST, Rz. 7 f. zu Art. 1 DSGVO.
[52] ERNST, Rz. 1 zu Art. 2 DSGVO.
[53] ERNST, Rz. 4 ff. zu Art. 2 DSGVO.
[54] ERNST, Rz. 10 zu Art. 2 DSGVO.

Der sachliche Anwendungsbereich enthält einige Ausnahmen gemäss Art. 2 Abs. 2 DSGVO. Liegt die Tätigkeit ausserhalb des Anwendungsbereichs des Unionrechts, so gilt auch die DSGVO nicht. Nach Erwägungsgrund 16 betrifft dies Tätigkeiten, die den Mitgliedsstaaten selbst überlassen sind, wie die nationale Sicherheit. Bei Tätigkeiten durch die Mitgliedsstaaten im auswärtigen Handeln der EU und den Bestimmungen der gemeinsamen Aussen- und Sicherheitspolitik, findet die DSGVO keine Anwendung, diese Fragen sind anhand von Art. 7 und 8 der Grundrechtscharta (GRCh)[55] zu beurteilen. Auch bei der Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung persönlicher oder familiärer Tätigkeiten, findet sie keine Anwendung.[56] Von dieser Ausnahme sind juristische Personen nicht erfasst. Diese Datenverarbeitung darf aber gemäss Erwägungsgrund 18 nur ohne jeglichen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden.[57] Bei der Verfolgung von Straftaten und der Strafvollstreckung findet die DSGVO ebenfalls keine Anwendung. Dadurch können die Mitgliedsstaaten frei über die Datenaufzeichnung für die Bekämpfung der Kriminalität verfügen. In diesen Fällen hat die Datenverarbeitung in den Schranken des nationalen Datenschutzes zu erfolgen.[58]

2.2.2 Räumlicher Anwendungsbereich

Art. 3 DSGVO regelt den räumlichen Anwendungsbereich. Da es beim Umgang mit Daten kaum eine Rolle spielt, wo die Landesgrenzen liegen, ist es wenig sinnvoll die rechtliche Anknüpfung an dem Ort der physischen Datenverarbeitung oder -speicherung zu haben.[59] Hat die datenverarbeitende Stelle ihren Sitz in der EU, so ist die DSGVO anwendbar. Es ist nicht relevant, ob die Daten technisch gesehen in der EU oder auf Servern ausserhalb der EU verarbeitet werden. Es ist auch unwesentlich, ob die Daten von Unionsbürgern sind oder Personen aus Drittstaaten.[60] Die DSGVO ist auch anwendbar für aussereuropäischen Unternehmen, für die in der EU vorhandenen Liegenschaften. Diese Anwendbarkeit der DSGVO auf aussereuropäische Unternehmen beschränkt sich aber nur auf die Datenverarbeitung der in der EU liegenden Niederlassung.[61] Auch auf innereuropäische Unternehmen, die ihre Daten mittels Outsourcings[62] in anderen Teilen der Welt

---

55 Charta der Grundrechte der Europäischen Union, C 326/395 vom 26.10.2012.
56 ERNST, Rz. 11 ff. zu Art. 2 DSGVO.
57 ERNST, Rz. 15 f. zu Art. 2 DSGVO.
58 ERNST, Rz. 22 zu Art. 2 DSGVO.
59 ERNST, Rz. 1 zu Art. 3 DSGVO.
60 ERNST, Rz. 3 f. zu Art. 3 DSGVO.
61 ERNST, Rz. 9 zu Art. 3 DSGVO.
62 Auslagerung von Tätigkeiten an einen Dienstleister, die ein Unternehmen selbst erbracht hat.

verarbeiten, findet die DSGVO ihre Anwendbarkeit. Es ist irrelevant, weshalb und wie die Datenverarbeitung ausserhalb von Europa vonstatten geht, da der Datenverantwortliche innerhalb der EU ist, untersteht er dem DSGVO. Für aussereuropäische Verarbeiter, die für eine innereuropäische Stelle oder als Subunternehmer eines innereuropäischen Auftraggebers agieren, ist sie ebenfalls anwendbar.[63]

Das Marktortprinzip von Art. 3 Abs. 2 DSGVO soll die EU-Bürger gemäss Erwägungsgrund 23 auch gegen ausserhalb der EU erfolgende Datenverarbeitungen schützen. Die DSGVO ist auch anwendbar, wenn ein aussereuropäisches Unternehmen mit ihrer Datenverarbeitung gezielt auf Personen in der EU eingeht. Dies ist bereits der Fall, wenn das Unternehmen Waren oder Dienstleistungen anbietet oder die Datenverarbeitung als Verhaltensbeobachtung fungiert. Wenn die Daten bloss durch einen innereuropäischen Router geleitet werden, ohne dass sie auf irgendeine Art und Weise verarbeitet werden, findet die DSGVO jedoch keine Anwendung.[64] Nach Abs. 3 findet die DSGVO ausserdem Anwendung auf die Verarbeitung von Personendaten «durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt». Betroffen sind hiermit diejenigen Orte, die nach Völkerrecht nicht dem Drittstaat angehören, in dem sie rein geographisch liegen. Insbesondere sind dies Konsulate oder diplomatische Vertretungen eines Mitgliedstaates in einem Drittland. Für die Datenverarbeitung an diesen Orten ist die DSGVO anwendbar.[65] Keine Anwendung hingegen findet die DSGVO in Drittländern. Als Drittländer gelten alle Staaten, die nicht Mitglied der EU sind, da die DSGVO nur für EU-Mitgliedsstaaten verbindlich ist. Island, Liechtenstein und Norwegen zählen jedoch nicht als Drittland, da diese beschlossen haben die DSGVO anzuwenden.[66]

2.2.3 Personenbezogene Daten

Der Begriff der personenbezogenen Daten ist im Datenschutzrecht fundamental. Er beinhaltet alle Informationen, die eine identifizierte oder identifizierbare natürliche Person betreffen. Identifizierte oder identifizierbare Person entspricht dem Begriff der bestimmten oder bestimmbaren Person. Bestimmbar ist eine Person, wenn sie mit direkten oder indirekten Merkmalen bestimmt werden kann. Dies passiert gemäss Art. 4 Nr. 1 DSGVO mittels Zuordnung zu einem Identifikator wie Namen, Kennnummer, Standortdaten,

---

63 ERNST, Rz. 11 f. zu Art. 3 DSGVO.
64 ERNST, Rz. 13 f. zu Art. 3 DSGVO.
65 ERNST, Rz. 21 zu Art. 3 DSGVO.
66 PAULY, Rz. 6 zu Art. 44 DSGVO.

Online-Kennung oder besonderen Merkmalen der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen kulturellen oder sozialen Identität. Es kann nur eine natürliche Person betroffen sein und dies nach Erwägungsgrund 27 nur während dem Zeitraum von Geburt bis Tod. Ein Schutz nach dem Tode kann aber aus anderen Gesetzen entstehen. Das DSGVO bezieht sich lediglich auf natürliche Personen. Das Datenschutzrecht ist nicht anwendbar bei reinen Unternehmensdaten oder Sachinformation, die nicht auch zur mittelbaren Identifizierung einer natürlichen Person geeignet sind.[67]

Es liegt ein personenbezogenes Datum vor, wenn eine Angabe einer bestimmten Person zugeordnet werden kann und ebenfalls, wenn der Betroffene mittels Referenzdaten ausgemacht werden kann. Bei absoluter Unmöglichkeit der Identifizierbarkeit, kann kein Zusammenhang zwischen einem Datum und einer natürlichen Person hergestellt werden und folglich fehlt es an der Bestimmbarkeit. Um zu ermitteln, ob eine natürliche Person identifizierbar ist, sollen gemäss Erwägungsgrund 26 «alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.» Unter allen Mitteln werden alle objektiven Faktoren wie Kosten und Zeitaufwand der Identifizierung verstanden. Zudem sind für die Identifizierung alle zum Verarbeitungszeitpunkt verfügbaren Technologien und technologischen Entwicklungen zu berücksichtigen. Im Hinblick auf die Technologien stellt sich die Frage, ob diese allgemein verfügbar sein müssen oder nur gegenüber dem Verantwortlichen. Dabei würde es sich um Zusatzwissen handeln, welches die Datenzuordnung zu einer Person vereinfachen könnte. Für die Beurteilung der Bestimmbarkeit ist es bereits ausreichend, dass ein solches Zusatzwissen zugänglich und erreichbar ist, unabhängig ob dies einen Aufwand generiert oder nicht. Potenziell personenbezogene Daten sind ebenfalls als bestimmbare Personendaten zu qualifizieren.[68]

Unter die personenbezogenen Daten fallen die persönlichen wie auch die sachlichen Angaben eines Betroffenen. Persönliche Angaben beziehen sich unmittelbar auf den Betroffenen, wie beispielsweise Name, Alter, Herkunft, Ausbildung, Fingerabdrücke, etc. Sachliche Angaben sind hingegen beispielsweise Angaben über die Beziehung der betroffenen Person gegenüber Dritten, der Umwelt oder ihr Kommunikationsverhalten. Weitere Personendaten sind unter anderem Geodaten, aufgrund ihrer Bestimmung von

[67] ERNST, Rz. 3 ff. zu Art. 4 DSGVO.
[68] ERNST, Rz. 8 ff. zu Art. 4 DSGVO.

Bewegungsprofilen, Auto-Complete-Daten, von Daten oder in Zusammenhang mit ihnen, oder Online-Identifikatoren wie IP-Adressen, sofern diese Daten ein Personenbezug haben. Grundsätzlich ist gemäss Art. 9 DSGVO die Verarbeitung von personenbezogenen Daten, aus denen die «rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person» verboten. Vorbehalten sind einige Ausnahmen nach Art. 9 Abs. 2 DSGVO.[69]

2.3 US-Cloud Act

Beim Clarifying Lawful Overseas Use of Data Act (US-Cloud Act)[70] handelt es sich um ein US-amerikanisches Bundesgesetz, ergänzend zum Stored Communications Act (SCA)[71], welches aufgrund des Microsoft Gerichtverfahrens im März 2018 erlassen wurde. Damals entschied der US-Court of Appeal zugunsten Microsoft, indem er beurteilte, der SCA habe keine exterritoriale Anwendung und Microsoft habe der US-Regierung deshalb zu Recht keine Daten aus ihren Servern in Irland herausgegeben.[72] Das U.S. Department of Justice (DOJ) zog die Angelegenheit weiter an den US-Supreme Court. Bevor dieser über die Sache urteilen konnte, verabschiedete der US-Kongress den Cloud Act, welcher den SCA änderte.[73]

2.3.1 Inhalt

Der Cloud Act soll den US-Strafbehörden bei der Verhütung, Ermittlung, Aufklärung oder Verfolgung von schweren Straftaten helfen. Er findet nur im Strafverfahren Anwendung.[74] Als schwere Straftaten werden explizit Terrorismus, erhebliche Gewaltverbrechen, Ausbeutung von Kindern, transnationales organisiertes Verbrechen oder erheblicher Finanzbetrug erwähnt.[75]

---

69 ERNST, Rz. 14 ff. zu Art. 4 DSGVO.
70 Clarifying Lawful Overseas Use of Data Act, A bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.
71 Stored Communications Act, 18 U.S. Code Chapter 121 - stored wire and electronic communications and transactional records access.
72 VASELLA, S. 1 f.
73 BJ, Bericht zum US-Cloud Act, S. 6.
74 BJ, Bericht zum US Cloud Act, S. 4.
75 § 2523 (b) (4) (H) Cloud Act.

Tangiert vom Cloud Act sind Gesellschaften, die der Gerichtsbarkeit der USA unterstellt sind.[76] Durch ihn werden die Anbieter von Kommunikationsdiensten (CSP) mit Sitz in den USA verpflichtet Daten, die sich in ihren Datenspeicherzentren befinden, aufzubewahren und den US-Strafverfolgungsbehörden auf Verlangen zu übergeben, auch wenn diese Zentren ausserhalb der USA sind.[77] Dadurch haben die USA einem nationalen Gesetz einen extraterritorialen Anwendungsbereich verleiht.[78]

2.3.2 Rechtshilfe

Grundsätzlich müssten die US-Behörden für im Ausland gespeicherte Daten ein zwischenstaatliches Rechtshilfegesuch stellen. Durch den Cloud Act ist dieses Rechtshilfegesuch jedoch nicht mehr notwendig, da ein direkter Zugang auf die Daten ermöglicht wird. Den Weg ohne Rechtshilfegesuch soll über bilaterale Executive Agreements, umsetzbar durch den Cloud Act, ermöglicht werden. Durch die Executive Agreements sollen die Strafverfolgungsbehörden der unterzeichnenden Staaten Zugang zu den jeweiligen Daten der CSP erhalten und diese direkt zu deren Ablieferung auffordern können.[79]

Zwischen den USA und der Schweiz besteht ein Staatsvertrag in Sachen Rechtshilfe[80]. Ersucht die Schweiz um Rechtshilfe so prüft das DOJ das Gesuch nach den allgemeinen Vorschriften des ersuchten Staates[81] und leitet es an die zuständige Behörde weiter. Es wird den Umständen entsprechend, so schnell als möglich ausgeführt.[82] Dies ist ein schwerfälliger Prozess, durch welchen die schweizerische Strafverfolgungsbehörde die ersuchten Beweismittel nicht immer zeitig erhalten hat.[83] Würde die Schweiz ein Executive Agreement mit den USA vereinbaren, könnten sich die schweizerischen Strafbehörden direkt an die CSP wenden, jedoch müssten sie doch den Rechtshilfeweg beschreiten, wenn das CSP die Datenherausgabe verweigern würde. Würde es jedoch mitwirken, so wäre die Zusammenarbeit wesentlich einfacher und schneller. Dies würde in einer

---

76 DOJ, S. 6 f.
77 §2713 Cloud Act.
78 BJ, Bericht zum US-Cloud Act, S. 5.
79 BJ, Bericht zum US-Cloud Act, S. 5.
80 Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vom 25. Mai 1973, SR 0.351.933.6.
81 Art. 9 Abs. 1 Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen.
82 Art. 31 Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen.
83 BJ, Bericht zum US Cloud Act, S. 5.

Entlastung der Rechtshilfe mit den USA resultieren, dadurch könnten sich die Behörden auf andere, nicht dem Cloud Act unterstehende, Fälle fokussieren.[84]

2.3.3 Executive Agreements

Seitens USA entscheidet der US Attorney General mit dem Aussenminister, ob der Staat die Abschlussanforderungen erfüllt und legt dem US-Kongress die schriftliche Argumentation vor.

Der Cloud Act stellt gewisse Anforderungen an den Staat, welcher mit den USA ein Executive Agreement abschliessen will.[85] Die nationale Gesetzgebung des potenziellen Vertragspartners muss hinsichtlich des Schutzes der Privatsphäre und der bürgerlichen Freiheiten im Hinblick auf die Datensammlung, solide materielle und verfahrensrechtliche Garantien gewähren. Im Besonderen muss er angemessene materielle und verfahrensrechtliche Gesetzesvorschriften im Gebiet der Cyberkriminalität und der elektronischen Beweismittel nachweisen können, dies kann er unter anderem, indem er Unterzeichner der Budapest-Konvention[86] ist. Generelle Anforderungen umfassen die Rechtsstaatlichkeit sowie den Grundsatz der Nichtdiskriminierung, sowie die Einhaltung der internationalen Menschrechte, insbesondere Schutz vor willkürlichen und rechtswidrigen Eingriffen in das Privatleben, das Recht auf ein faires Verfahren, Meinungs- und Versammlungsfreiheit, Verbot der willkürlichen Festnahme oder Inhaftierung, wie auch Folterverbot und grausame, unmenschliche oder erniedrigende Behandlung oder Strafe.

Die aufgrund des Executive Agreements Daten ersuchenden Behörden, müssen klare, rechtlich definierte Mandate haben und über eine gesetzliche Grundlage bei der Erhebung, Speicherung, Verwendung und Bekanntgabe der Daten verfügen. Die Erhebung und Nutzung der Daten müssen der ausländischen Regierung transparent nachgewiesen werden. Ausserdem muss der Vertragspartner belegen, dass er engagiert ist, den freien globalen Datenverkehr und das offene, vernetzte Wesen des Internets zu schützen.[87]

Unter dem Cloud Act darf die ausländische Herausgabeanordnung keine Daten einer US-Person betreffen.[88] Eine US-Person umfasst Staatsbürger der Vereinigten Staaten, Ausländer mit ständigem Wohnsitz in den USA oder juristische Personen der amerikanischen

---

84 BJ, Bericht zum US Cloud Act, S. 6.
85 § 2523 (b) Cloud Act.
86 Übereinkommen über die Cyberkriminalität vom 23. November 2001, SR 0.311.43.
87 § 2523 (b) (1) (B) Cloud Act.
88 § 2523(b) (4) Cloud Act.

Gerichtsbarkeit, folglich mit Sitz in den USA.[89] Im Umkehrschluss darf die US-Strafverfolgungsbehörde nicht die Datenherausgabe von Personen mit schweizerischer Staatsangehörigkeit, Wohnsitz in der Schweiz oder juristischen Personen mit Sitz in der Schweiz verlangen. Es dürfen demnach von ausländischen Behörden keine Anordnungen, welche direkt oder indirekt eine US-Person betreffen gestellt werden.[90] Handelt es sich um Personendaten, welche vom Anwendungsbereich des Executive Agreements nicht umfasst werden, so muss ein Rechtshilfegesuch gestellt werden.[91]

Wie bereits ausgeführt muss die Datenherausgabe aufgrund einer schweren Straftat angeordnet werden. Die Anordnung soll eine gezielte Person, samt Adresse, persönlichem Gerät oder anderem spezifischen Identifizierungsmerkmal erfassen, mit dem Recht des anordnenden Staates konform sein und durch glaubwürdige Fakten begründet sein. Zudem muss sie durch Gerichte oder andere unabhängige Behörden überprüfbar sein sowie, im Falle einer Abhörung, befristet und verhältnismässig sein.[92]

2.3.4 Territorialität

Das Territorialitätsprinzip umfasst das Gebiet, innerhalb der durch Völkerrecht vereinbarten oder anerkannten internationalen Grenzen.[93] Es weist eine enge Verbindung auf zur Staatssouveränität. Diese beinhaltet die Kompetenz der Staaten, sich in rechtlicher und struktureller Hinsicht selbst zu organisieren und internationale Verträge abzuschliessen, andererseits umfasst es das Verbot sich in die Intima anderer Staaten einzumischen, das so genannte Interventionsverbot.[94] Durch das Territorialitätsprinzip und dem Interventionsverbot erschliesst sich das Verbot für die Staaten, durch ihre Rechtsordnung oder ihre effektiven Handlungen die Souveränität oder Territorialität anderer Staaten zu verletzen.[95]

Im Lotus-Fall von 1927[96], Frankreich gegen die Türkei, entschied der Ständige Internationale Gerichtshof (StIGH), dass durch das Territorialitätsprinzip Rechtsanwendungen, die über das eigene Hoheitsgebiet hinausgehen, dann nicht ausgeschlossen sind, wenn sie

---

89 31 CFR § 560.314.
90 § 2523 (b) (4) Cloud Act.
91 BJ, Bericht zum US Cloud Act, S. 10.
92 § 2523 (b) (3) (D).
93 BESSON/BREITENMOSER/PETRIG/SASSÒLI/ZIEGLER, S. 162.
94 Art. 2 Abs. 7 UNO-Charta.
95 BJ, Bericht zum US-Cloud Act, S. 16.
96 CPJI vom 07.09.1927, Affaire du «Lotus», Série A - No. 10, S. 18 f.

völkerrechtlich nicht ausdrücklich unzulässig sind.[97] Die Globalisierung und insbesondere die moderne Kommunikation, durch welche Daten global jederzeit verfügbar und abrufbar sind, stellen das Territorialitätsprinzip nicht generell in Frage. Jedoch vermehren sich die Berührungspunkte und dadurch das Potential zum Zusammenstoss von Rechtsordnungen verschiedener Staaten.[98]

Aufgrund der signifikanten Rolle der staatlichen Behörden im Strafrecht, ist derjenige Staat zuständig für die Beweiserhebung, auf welchem sich die Beweismittel territorial befinden. Wo die Beweismittel liegen, ist daher von grosser Bedeutung. Dies wurde auch für Daten bisher analog gehandhabt, demnach ist zu schliessen, dass die Beweismittelerhebung von Daten an deren Lageort zu folgen hat.[99] Unter den Geltungsbereich des Cloud Acts fallen wie bereits ausgeführt, alle CSP mit Sitz in den USA.[100] Wenn ein ausländisches CSP in den USA Geschäftsniederlassungen hat, so findet der CSP auch auf sie und ihre Daten Anwendung, auch wenn diese ausserhalb der USA gespeichert sind. Der Cloud Act schliesst nicht aus, dass Nicht-US-CSP, die aber am US-Markt auftreten vom Cloud Act ausgenommen sind.[101] Daraus folgt, dass die US-Strafverfolgungsbehörden aufgrund des Cloud Acts auch Daten erheben können, die nicht in ihrem Hoheitsgebiet liegen und sich an CSP wenden können, die nicht der amerikanischen Gerichtsbarkeit unterliegen. Dass sich die US-Behörden gestützt auf den Cloud Act direkt auf Personen, also CSP, im Hoheitsgebiet eines anderen Staates wenden können, kann betreffend der Territorialität problematisch werden. Der Cloud Act kann demnach durch seinen Anwendungsbereich zu extraterritorialen strafrechtlichen Kompetenzdisputen führen.[102]

3 Rechtsvergleich

3.1 Verhältnis US-Cloud Act mit der DSGVO

Wie bereits ausgeführt gelten die Bestimmungen der DSGVO auch für Schweizer Unternehmen, wenn sie in den Geltungsbereich nach Art. 3 DSGVO fallen.[103] Bei CSP ist dies insbesondere der Fall, wenn er seine Niederlassung innerhalb der EU hat oder falls die Niederlassung nicht in der EU ist, eine Datenbearbeitung im Zusammenhang mit EU-

97 BESSON/BREITENMOSER/PETRIG/SASSÒLI/ZIEGLER, S. 158.
98 BJ, Bericht zum US-Cloud Act, S. 16.
99 BJ, Bericht zum US-Cloud Act, S. 17.
100 Vgl. Kapitel 2.3.1.
101 Nationalversammlung Frankreich, S. 29 f.
102 BJ, Bericht zum US Cloud Act, S. 17 f.
103 Vgl. Kapitel 2.2.2.

Personen erfolgt oder deren Verhalten beobachten wird, sofern dieses in der EU erfolgt. Gestützt auf Art. 6 DSGVO i.V.m. Art. 49 DSGVO kann es in Ausnahmefällen gerechtfertigt werden, dass Datenbearbeitungen in einem Drittstaat stattfinden, auch wenn dieser weder einen Angemessenheitsbeschluss der Europäischen Kommission hat noch über spezifische Garantien nach Art. 46 DSGVO verfügt. Der Angemessenheitsbeschluss wird durch die europäische Kommission auf Basis von Art. 45 DSGVO gefällt, wenn das betroffene Drittland ein angemessenes Datenschutzniveau bietet. Ein solcher Ausnahmefall würde vorliegen, wenn ein CSP Personendaten «zum Schutz der lebenswichtigen Interessen der betroffenen Person» bekannt gibt nach Art. 6 Abs. 1 lit. d DSGVO i.V.m. Art. 49 Abs. 1 lit. f DSGVO. Oder wenn eine derartige Datenbekanntgabe durch ein anerkanntes öffentliches Interesse der EU und ihren Mitgliedsstaaten gerechtfertigt werden kann, etwa bei konkreten Indizien eines terroristischen Anschlags oder eines schweren Straftatbestands gemäss Art. 49 Abs. 1 lit. d DSGVO. Deshalb ist jedoch die Rechtmässigkeit der Datenbearbeitungen gestützt auf die Herausgabeanordnungen der US-Behörden im Sinne des Cloud Acts als problematisch zu qualifizieren. Denn die Datenbekanntgabe ist nur in absoluten Ausnahmefällen erlaubt, da die Rechte und Freiheiten der betroffenen Person dadurch stark eingeschränkt werden.[104]

Auch im Hinblick auf die Transparenz ist der Cloud Act ebenfalls als bedenklich zu beurteilen. Die US-Strafverfolgungsbehörden müssen die betroffene Person nicht in jedem Fall über die Datenbekanntgabe informieren und können die CSP mittels gerichtlicher Verfügung gar anordnen, die Information an die betroffene Person zu unterlassen.[105] Jedoch ist die Information an die betroffene Person über beantragte Datenzugänge von Strafverfolgungsbehörden im europäischen Recht unentbehrlich.[106]

Der Grundsatz der Verhältnismässigkeit wird mit dem Cloud Act eingehalten.[107] Denn die US-Strafverfolgungsbehörde, welche die Datenbekanntgabe verlangen will, kann dies nur tun, wenn ein Gericht die Herausgebe vorab genehmigt hat und die Behörde ausreichend dargelegt hat, dass ein geeigneter Verdacht besteht, dass ein bestimmtes Verbrechen stattgefunden hat oder stattfinden wird und die verlangten Informationen Beweise für ebendieses Verbrechen darstellen. Zudem muss die Behörde genau bestimmen,

[104] BJ, Bericht zum US-Cloud Act, S. 23 f.
[105] 18 U.S. Code § 2703(b)1.
[106] EDPB, Stellungnahme 23/2018, S. 19.
[107] EDPS/EDPB, S. 2.

welche Personendaten bekanntzugeben sind, fishing expeditions sind unzulässig.[108] Eine fishing expedition ist eine verbotene Beweisausforschung.[109]

Da der Cloud Act zwischen Daten von US-Persons und anderen Personen unterscheidet[110] und die DSGVO die Personendaten aller natürlichen Personen im gleichen Umfang schützt, erscheint hier ein Problem in der Übereinstimmung des Schutzbereichs dieser zwei Rechtsordnungen.[111] Jede Ungleichbehandlung aus datenschutzrechtlicher Sicht aufgrund der Ansässigkeit oder Staatsangehörigkeit der betroffenen Person ist im Sinne der DSGVO unzulässig.[112] Zudem sieht der Cloud Act keine Auskunftsrechte für betroffene Personen hinsichtlich ihrer Personendaten vor, was dem Grundrecht aus Art. 8 Abs. 2 GRCh widerspricht, welches das Recht auf Auskunft explizit garantiert. Wird eine Herausgabeanordnung ausgesprochen, so hat die betroffene Person unter dem Cloud Act weder eine Beschwerdemöglichkeit an eine unabhängige Aufsichtsbehörde noch Anspruch auf einen gerichtlichen Rechtsbehelf gegen die Datenbekanntgabe. Das Fehlen dieses Rechtsbehelfes steht im Gegensatz zu Art. 47 GRCh, welches das Recht auf wirksamen gerichtlichen Rechtsschutz gewährt. Basierend auf diesen Ausführungen, ist die Vereinbarkeit vom Cloud Act und der DSGVO als problematisch einzustufen.[113]

3.1.1 Safe-Harbor

Die Europäische Kommission hat im Jahre 2000 die Entscheidung 2000/520[114] erlassen. Mit dieser Entscheidung haben sie anerkannt, dass die Regeln, welche zwischen der EU und den USA ausgehandelt wurden, das Datenschutzniveau gewährleisten. Daraus durften personenbezogene Daten aus der EU an Unternehmen der USA weitergeleitet werden, ohne das europäisches Datenschutzrecht verletzt wird, sofern die Unternehmen die Safe-Harbor-Grundsätze anwenden.[115] Die Safe-Harbor-Regelungen enthalten die Voraussetzungen der innerstaatlichen Rechtsvorschriften sowie internationalen Verpflichtungen für eine Anerkennung als Drittland mit einem angemessenen Datenschutzniveau, wodurch die Datenlieferung aus den EU-Mitgliedstaaten ohne weitere Anforderungen an

[108] DOJ, S. 8.
[109] Urteil des Bundesverwaltungsgerichts, A-1735/2011 vom 21 Dezember 2011, E. 3.3.
[110] Vgl. Kapitel 2.3.4
[111] BJ, Bericht zum Cloud Act, S. 25.
[112] EDPS, Stellungnahme 2/2019, Rz. 50.
[113] BJ, Bericht zum Cloud Act, S. 25.
[114] Entscheidung der Kommission vom 26. Juli 2000, 2000/520/EG.
[115] SIDLER/VASELLA, S. 186.

ebendieses Drittland geschehen kann.[116] Auch die Schweiz schloss mit den USA ein vergleichbares Safe-Harbor Abkommen im Jahre 2009.[117]

Im Juni 2013 legte Maximilian Schrems, österreichischer Jurist und Datenschutzaktivist, Beschwerde beim Datenschutzbeauftragten in Irland ein. Seine Beschwerde richtete sich gegen die Übermittlung seiner personenbezogenen Daten von Facebook Irland (Tochtergesellschaft von Facebook) an Facebook USA (Muttergesellschaft).[118] Herr Schrems forderte den Datenschutzbeauftragten auf, die Übermittlung der personenbezogenen Daten von Facebook Irland in die USA zu verbieten. Dies mit der Begründung, dass die Vereinigten Staaten mit ihrem Recht und ihrer Praxis keinen ausreichenden Schutz gespeicherter Personendaten vor den Überwachungen der dortigen Behörden gewährleisten. Er bezog sich auf die Tätigkeiten der amerikanischen Nachrichtendienste, namentlich diese der National Security Agency (NSA).

Der Datenschutzbeauftragte Irlands vertrat die Meinung, es gäbe keinerlei Beweise für einen solchen Zugriff der amerikanischen Behörden auf die Personendaten von Herr Schrems. Zudem weise die USA ein angemessenes Schutzniveau auf, verweisend auf das Safe-Harbor Abkommen. Die abgewiesene Beschwerde zog Herr Schrems mittels Klage weiter zum irischen High Court.[119] Dieser legte dem Gerichtshof der Europäischen Union (EuGH) folgende zwei Fragen zur Vorabentscheidung vor, da es sich dabei um die Durchführung von Unionsrecht handelte im Sinne von Art. 51 GRCh.[120]

1. Ist eine nationale Datenschutzbehörde bei der Beschwerdeprüfung, bezüglich der Angemessenheit des Schutzniveaus eines Drittlandes, im Hinblick auf Art. 7, 8 und 47 GRCh, absolut an die Kommissionsentscheidung und ihre gegenteilige Feststellung gebunden?

---

116 WIDMER, S. 148.

117 Briefwechsel vom 1. und 9. Dezember 2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika, SR 0.235.233.6.

118 WIDMER, S. 148.

119 EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 28 ff.

120 EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 34.

2. Oder kann und/oder muss die nationale Datenschutzbehörde eigene Ermittlungen in der Sache anstellen mit Blick auf die tatsächlichen Entwicklungen seit der Veröffentlichung des Entscheids der Kommission?[121]

Das EuGH nimmt auf die vorgelegten Fragen Stellung, indem es entscheidet, dass die nationale Kontrollstellen des Datenschutzes der Mitgliedsstaaten verpflichtet sind, die Vereinbarkeit einer Kommissionsentscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte der betroffenen Person mit aller gebotenen Sorgfalt zu prüfen.[122] Der Gerichtshof begründet dies damit, dass eine Entscheidung der Kommission, wie Safe-Harbor, eine betroffene Person, deren Personendaten in ein Drittland übermittelt werden, sie nicht daran hindern könne, eine Kontrollstelle mit einer Eingabe zur Prüfung zu beschäftigen. Zudem könne eine solche Entscheidung, die den Kontrollstellen zugeteilten Befugnisse weder beseitigen noch eingrenzen. Ansonsten würde den Personen, deren Daten in das Drittland übermittelt wurden oder werden könnten, das Recht aus Art. 8 GRCh verweigert, sich zum Schutze ihrer Grundrechte an die Kontrollstellen zu wenden.[123]

Obiter dictums beantwortet der EuGH die Fragestellung nach der Gültigkeit der Safe-Harbor Entscheidung der Kommission. Er begründet diese Vorgehensweise damit, dass das Gericht die Zweifel von Herrn Schrems über die Gültigkeit der Entscheidung teilt. Zu prüfen sei daher, ob Safe-Harbor im Lichte der Charta die Anforderungen der Datenschutzrichtlinie 95/46[124] erfüllt.[125] In diesem Rahmen setzt sich der Gerichtshof mit dem Begriff «angemessenes Schutzniveau» auseinander. Er kommt zum Schluss, dass das Wort «angemessen» zwar nicht verlangt, dass ein Drittland ein garantiert kongruentes Schutzniveau wie die Europäische Union hat, aber es wird verlangt, dass das Drittland mit seinen Rechtsvorschriften und internationalen Verpflichtungen faktisch ein Schutzniveau gewährleistet, dass dem in der Union aufgrund der Richtlinie garantieren Stufe gleichwertig ist. Ohne dieses Erfordernis könnte, dem in der Union garantierten, hohen

---

[121] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 36.
[122] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 63.
[123] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 66.
[124] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31.
[125] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 67.

Schutzniveau leicht ausgewichen werden, dadurch das personenbezogene Daten aus der EU in Drittländer übermittelt würden, damit sie dort verarbeitet werden.[126]

Während der Prüfung der Safe-Harbor-Regelungen stellt der Gerichtshof ausserdem fest, dass Bearbeitungen von personenbezogenen Daten unbedingt den Kriterien von Art. 7 GRCh (Achtung des Privat- und Familienlebens, insbesondere der Kommunikation), Art. 8 GRCh (Schutz personenbezogener Daten), Art. 47 GRCh (Recht auf wirksamen Rechtsbehelf und ein unparteiisches Gericht) und Art. 52 Abs. 1 GRCh (Voraussetzungen für Grundrechtseingriffe) entsprechen müssen.[127] Eine Regelung, durch welche Behörden generell auf den Inhalt elektronischer Kommunikation zugreifen können, verletzt den Kerngehalt des Grundrechts auf Achtung des Privatlebens gemäss Art. 7 GRCh.[128] Basierend auf diesen Erkenntnissen urteilte der EuGH, dass die Kommission mit ihrer Entscheidung 2000/520 keine ausreichenden Gründe belegen kann mit denen die USA beruhend auf innerstaatliche Rechtsvorschriften oder internationale Verpflichtungen nach Art. 25 Abs. 6 der Richtlinie 95/46 ein angemessenes Schutzniveau gewährleisten würden. Folglich sei die Entscheidung der Kommission und damit das Safe-Harbor-Abkommen mit den USA ungültig.[129]

3.1.2 Privacy Shield

Zum Zeitpunkt des Schrems I Urteils liefen die Verhandlungen über ein revidiertes Datenschutzabkommen zwischen der EU und den USA bereits.[130] Die Parteien haben sich am 2. Februar 2016 auf das Wesentliche eines revidierten Abkommens[131] geeinigt, welches als EU-US Privacy Shield bekannt wurde. Es handelt sich beim Privacy Shield, wie zuvor beim Safe-Harbor-Abkommen um kein eigentliches Abkommen, sondern um Handlungen und Versprechen der USA, mit welchen die Kommission die Angemessenheit des amerikanischen Datenschutzniveaus prüfen soll.[132]

---

[126] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 73.
[127] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 91 ff.
[128] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 94.
[129] EUGH vom 06.10.2015, Rs. C-363/14, Maximillian Schrems gegen Data Protection Commissioner, Rz. 105 f.
[130] Memo, S. 3 ff.
[131] Medienmitteilung EU-US Privacy Shield, S. 1 f.
[132] SIDLER/VASELLA, S. 189 f.

Das Privacy Shield hält folgende Schwerpunkte fest, die zur Datenschutzverbesserung beisteuern sollen:

- US-Unternehmen, welche personenbezogene Daten verarbeiten dürfen, müssen sich nach ihrer Zertifizierung an strengere Regeln halten. Neu gibt es besondere Informationspflichten, Opt-Out-Rechte der betroffenen Personen, Regelungen zur Weitergabe von Personendaten, Auflagen zur Datensicherheit, Bestimmungen zur Verhältnismässigkeit, Zweckbindung und Datenqualität bei der Erhebung von Daten, grundsätzliche Anordnungen zum Auskunftsrecht der betroffenen Personen und zum Rechtsschutz.[133]

- Ob die US-Unternehmen den Auflagen nachkommen, soll besser kontrolliert und durchgesetzt werden. Die Unternehmen, welche sich zur Einhaltung der Privacy Shield Grundsätze verpflichten, müssen die Grundsätze vollständig einhalten und werden bezüglich der Publikation ihrer Verpflichtungen vom US-Handelsministerium überwacht. Die Federal Trade Commission (FTC) kontrolliert die Einhaltung der Grundsätze.[134] Bei Verstössen sind Sanktionen bestimmt und fehlbare Unternehmen können ihre Zertifikation verlieren. Das FTC hat sich dazu verpflichtet, Beschwerden von EU-Mitgliedsstaaten bezüglich dem Privacy Shield Priorität zu behandeln.[135]

- Es sollen neue Schutzvorkehrungen beim Datenzugriff durch US-Behörden gelten. Werden Daten widerrechtlich und absichtlich benutzt oder bekannt gemacht, so haften die USA für den Schaden. Es steht auch Nicht-US-Personen frei, Ansprüche gegen Mitglieder der US-Behörden wegen widerrechtlicher Überwachung geltend zu machen.[136] Ausserdem wird eine Ombudsperson beschäftigt und ein Koordinationsverfahren hervorgerufen.[137]

Die Kommission hält in ihrem Entscheid fest, dass der Privacy Shield in Übereinstimmung mit dem Urteil Schrems I des EuGH sei.[138]

---

133 Commission implementing Decision Privacy Shield, Rz. 16 ff.
134 U.S. Department of Commerce, Annex II, Ziff. I.2.
135 U.S. Department of Commerce, Annex II, Ziff. II.7.
136 Director of National Intelligence, Annex VI, Ziff. I.
137 US Secretary of State John Kerry, Annex III, S. 2 ff.
138 Entscheidung vom 29.02.2016, S. 6.

3.1.3 Urteil EuGH / Schrems II

Am 16. Juli 2020 entschied der EuGH zum zweiten Mal nach dem Schrems I Urteil im Jahre 2015 über eine Beschwerde von Herrn Maximilian Schrems. Folglich zum ersten EuGH-Urteil machte Facebook Irland geltend, sie würden die personenbezogenen Daten ihrer Nutzer auf Grundlage der gültigen EU-Standardvertragsklauseln in die USA übermitteln. Der EuGH beantwortete in seiner Entscheidung wesentlich Fragen über die Gültigkeit des Privacy Shields, die Gültigkeit der Standardvertragsklauseln sowie deren erforderliches Schutzniveau bei der Übermittlung und über die Befugnisse der Aufsichtsbehörden.[139]

Gemäss dem EuGH stellen die Regelungen des Privacy Shields kein Datenschutzniveau dar, dass dem europäischen gleichwertig sei. Daher erklärte er den Kommissionsbeschluss über das Privacy Shield als ungültig.[140]

Der EuGH hegt Zweifel an den von der Kommission geprüften Umständen, mit welchen sie im Ausgangsverfahren das amerikanische Recht für angemessen in Anbetracht auf das erforderliche Schutzniveau nach Art. 45 DSGVO in Verbindung mit den Grundrechten aus Art. 7, 8 und 47 der GRCh befanden. Insbesondere ist der Gerichtshof der Ansicht, dass die USA hinsichtlich der von ihrem nationalen Recht erlaubten Eingriffe nicht die erforderlichen Einschränkungen und Garantien vorsieht und auch keinen effektiven gerichtlichen Rechtsschutz gegen ebendiese Eingriffe sicherstellt. Eine Ombudsperson des Privacy Shields entspricht nicht einem gerichtlichen Rechtsschutz, da diese nicht gleich zu setzen ist wie ein Gericht nach Art. 47 GRCh.[141] Wie bereits ausgeführt muss die Kommission die Einhaltung des in der europäischen Union erforderliche Schutzniveau prüfen, bevor sie ein Angemessenheitsbeschluss erlässt. Dabei muss das Drittland insbesondere den Schutz der Rechte von Art. 7 und 8 GRCh garantieren. Die Kommission stellte fest, die Einsetzung einer Ombudsperson würde den von der Kommission selbst festgestellten Defiziten des gerichtlichen Rechtsschutzes von Personen, deren personenbezogenen Daten in die USA transferiert werden abhelfen. Der Gerichtshof konnte diese

[139] STRASSEMEYER/SCHEFZIG/MOOS, Rz. 97.
[140] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 201.
[141] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 168.

Schlussfolgerung nicht nachvollziehen und entschied, dass durch das Einsetzen einer Ombudsperson kein angemessenes Schutzniveau der Vereinigten Staaten gewährleisten werden kann.[142]

Nach Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten nur «für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage» verarbeitet werden. Eine Einschränkung eines solchen Grundrechts ist zwar möglich, jedoch muss diese gemäss Art. 52 Abs. 1 Satz 1 GRCh gesetzlich vorgesehen sein und den Kerngehalt dieser Rechte und Freiheiten ist achten. Einschränkungen der Rechte und Freiheiten dürfen nach Art. 52 Abs. 1 Satz 2 GRCh unter dem Grundsatz der Verhältnismässigkeit nur vorgenommen werden, sofern sie erforderlich sind und den von der Union anerkannten Gemeinwohl dienenden Ziele oder Erfordernisse des Schutzes der Rechte und Freiheiten anderer entsprechen. Der Eingriff ist nur verhältnismässig, wenn sich die Einschränkungen des Schutzes personenbezogener Daten auf das absolut Notwendige beschränken und klare, präzise Regeln für die Tragweite und Anwendungen sowie die Mindestanforderungen bestehen, damit die Personen, deren Daten transferiert werden, über einen genügenden Schutz ihrer Daten vor Missbrauchsrisiken verfügen.[143] Die Gewährleistung dieser Garantien ist bei automatisch verarbeiteten Personendaten umso bedeutsamer.[144]

Im Gegensatz zum Privacy Shield hält der Gerichtshof die Standardvertragsklauseln aufrecht.[145] Er hält es aber für angemessen, dass das verlangte Datenschutzniveau aus Art. 44 und Art. 46 DSGVO beim Datentransfer in ein Drittland einzelfallabhängig geprüft wird. Art. 46 DSGVO präzisiere zwar nicht die Art der Anforderungen des Datenschutzniveaus, jedoch ist es ein Teil von Kapital V «Verhaltensregeln und Zertifizierung» der DSGVO und daher im Lichte von Art. 44 DSGVO anzusehen ist. Dieser besagt; «Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird». Dieses Schutzniveau muss demnach garantiert werden, unabhängig davon, aufgrund welches Artikels aus Kapitel V eine Übermittlung von Personendaten in ein

[142] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 190.
[143] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 173 ff.
[144] EuGH vom 08.04.2014, Rs. C-293/12 und C-584/12, Digital Rights Ireland Ltd, Rz. 55.
[145] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 149.

Drittland erfolgt.[146] Daraus schliesst der EuGH, dass Unternehmen selbst prüfen müssen, ob sie für diejenigen Personen, deren personenbezogenen Daten mittels Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein solches Schutzniveau gewährleisten, das dem garantieren Schutzniveau der europäischen Union gleichwertig ist.[147] Die Gültigkeit der Standardvertragsklauseln hängt davon ab ob sie die relevanten Mechanismen, aus den aus Art. 46 DSGVO in Verbindung mit Art. 7, 8 und 47 GRCh resultierenden Ansprüchen enthalten, damit sie die DSGVO einhalten können oder, wenn gegen die Klauseln verstossen wird oder die Einhaltung nicht möglich ist, die Übermittlung von personenbezogenen Daten ausgesetzt wird.[148]

Es kann für die Unternehmen erforderlich sein, dass sie zusätzliche Massnahmen für die Gewährleistung des Schutzniveaus ergreifen müssen. Dies, da die Standardvertragsklauseln das Ziel verfolgen, diejenigen Garantien zu bieten, die in allen Drittländern übereinstimmend gelten, unabhängig von dem garantierten Schutzniveau des jeweiligen Drittlandes. Es kann also aufgrund der Schutzniveaus des Drittlandes erforderlich sein, zusätzliche Massnahmen zu vereinbaren.[149] Die zuständige Aufsichtsbehörde kann anweisen, dass Datenübertragungen in ein Drittland auszusetzen seien, oder sie kann diese gar verbieten, wenn die Behörde der Ansicht ist, dass die Standardvertragsklauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können.[150]

Das Urteil stellt nicht nur die Ungültigkeit des Privacy Shields, sondern auch die Gültigkeit der Standardvertragsklauseln fest. Durch seine Ausführungen zum erforderlichen Datenschutzniveau ist es für Unternehmen für fast jede Art von Personendatenübermittlung in Drittstaaten relevant.[151]

---

[146] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 92.
[147] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 96.
[148] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 135 ff.
[149] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 133.
[150] EuGH vom 16.07.2020, Rs. C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems, Rz. 113.
[151] STRASSEMEYER/SCHEFZIG/MOOS, Rz. 107.

3.1.4 Folgen des Urteils für die Schweiz

Die Schweiz hat im Januar 2017, in den letzten Tagen der Präsidentschaft des ehemaligen US-Präsident Barack Obama, mit den USA ein Privacy Shield Agreement abgeschlossen. Dabei handelte es sich um einen Austausch von unilateralen Erklärungen beider Regierungen, welches in seinem Inhalt dem EU-US Privacy Shield sehr ähnlich ist. Infolgedessen stellte sich die Frage ob und inwiefern das Schrems II Urteil des EuGH Konsequenzen für die Schweiz mit sich trägt.[152] Da die Schweiz jedoch nicht als EU-Mitgliedsstaat zählt, ist das Urteil des EuGH nicht rechtlich verbindlich.[153]

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) der Schweiz führt eine Staatenliste[154] mit Ländern welche einen angemessenen Schutz im Sinne von Art. 6 Abs. 1 DSG (Art. 16 nDSG) garantieren. Die USA hat noch nie zu der Gruppe dieser Staaten gehört, weshalb beim Transfer von Personendaten aus der Schweiz in die USA die Schutzmassnahmen nach Art. 6 Abs. 2 DSG (Art. 16 Abs. 2 nDSG) zu gewährleisten sind.[155] Nach dem heute geltenden Recht kann ein angemessener Schutz durch Vertrag, Einwilligung, bei Bearbeitung von Personendaten des Vertragspartners in Zusammenhang mit dem Vertragsabschluss oder im Einzelfall für die Wahrung eines überwiegenden öffentlichen Interessens garantiert werden. Andere Gründe der Garantie liegen vor, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen, bei Zugänglichmachen der Daten durch die betroffene Person oder bei Bekanntgabe innerhalb derselben juristischen Gesellschaft. Nach dem nDSG wird ein angemessener Schutz gewahrt durch völkerrechtlichen Vertrag, Datenschutzklauseln in einem Vertrag, die dem EDÖB vorgängig mitgeteilt wurden, spezifische Garantien eines zuständigen Bundesorgans, Standarddatenschutzklauseln oder verbindliche unternehmensinterne Datenschutzvorschriften, die vom EDÖB genehmigt wurden. Für die USA wurde ein teilweise angemessenes Datenschutzniveau angenommen.[156] Es handelte sich um eine partielle Annahme, da sie sich nur auf den Datenaustausch mit denjenigen US-Unternehmen begrenzte, die ein Zertifizierungsverfahren durchlaufen haben, welches die USA der Schweiz und der EU hinsichtlich des Privacy Shields mit nahezu identischen Regeln separat garantiert haben. Das Privacy Shield sah einen alljährlichen Joint Review zur Evaluierung der Funktionsweise vor. Die Reviews fanden jeweils anschliessend an die Joint

[152] WEBER, Datenexport in die USA, S. 25.
[153] EDÖB, Stellungnahme, S. 5.
[154] EDÖB, Staatenliste.
[155] EDÖB, Stellungnahme, S. 2.
[156] EDÖB, Staatenliste, S. 12.

Reviews der Vertreter der Europäischen Kommission und des Europäischen Datenschutzausschusses statt, bei welchen die Schweiz als Beobachter beiwohnend war.[157] Der EDÖB behielt sich das Recht vor, durch die Joint Reviews den Listenplatz der USA anzupassen, sollte dies aufgrund der gewonnenen Erkenntnisse als angebracht erscheinen. Er berücksichtigte bei seiner Evaluation die Rechtsprechung der Schweizer Gerichte wie auch diese der EU.[158]

Wie bereits ausgeführt hat der EuGH das Verhältnis von US-Überwachungsmassnahmen und dem Grundrecht auf Datenschutz ausschliesslich in Relation von Art. 7 und 8 GRCh prüfen können. Der EDÖB hingegen hat in seiner Stellungnahme das Spannungsfeld zwischen dem Recht auf Privatsphäre nach Art. 13 BV und möglichen Einschränkungen dieses verfassungsmässigen Rechts kaum behandelt.[159] Obwohl das Urteil des EuGH für die Schweiz nicht rechtlich verbindlich ist, wird das Datenschutzrecht der EU und daraus folgend auch die Rechtsprechung des europäischen Gerichthofes von den Behörden und Gerichten der EU auch gegenüber Schweizer Unternehmen angewendet.

Dies ergibt sich aus Art. 3 der DSGVO in welchem der räumliche Geltungsbereich auch gegenüber Schweizer Unternehmen Anwendung findet, sofern diese Daten von betroffenen Personen bearbeiten, die sich in der EU befinden, um den Personen Waren und Dienstleistungen anzubieten oder deren Verhalten zu beobachten, sofern dieses in der EU erfolgt. Schweizer Unternehmen müssen damit rechnen, dass sie von ausländischen Behörden aufgefordert werden sich an das EU-Recht zu halten. Da kein Schweizer Gericht eine ähnliche Rechtsfrage wie diese im EuGH Urteil behandelte, ist noch unklar zu welchen Schlüssen die Schweizer Rechtsprechung gelangen würde. Deshalb entschloss sich der EDÖB den Listenplatz der USA neu zu beurteilen und die allfällige Anpassung rechtlich zu begründen, dies mit Achtung des Prinzips der Rechtsstaatlichkeit und dem Interesse an Rechtssicherheit.[160]

Der EDÖB schätzt den Mangel an Transparenz an der Wirksamkeit einer Ombudsperson, durch welche einen indirekt durchsetzbaren Rechtsbehelf garantiert sein soll und deren tatsächliche Unabhängigkeit gegenüber den US-Geheimdiensten sowie die daraus abzuleitende Abwesenheit von Garantien bei Eingriffen der US-Behörden in die Privatsphäre

[157] EDÖB, Stellungnahme, S. 2.
[158] EDÖB, Mitteilung.
[159] EDÖB, Stellungnahme.
[160] EDÖB, Stellungnahme, S. 5.

von Personen in der Schweiz als unverträglich dar. Dieser Mangel kann mit der Rechtsweggarantie nach Art. 29 ff. BV und Art. 15 DSG (Art. 32 nDSG) in Verbindung mit dem Schutz der Privatsphäre gemäss Art. 13 Abs. 2 BV sowie den aus Art. 8 EMRK garantierten Rechte auf Achtung des Privat- und Familienlebens und den Grundsätzen der rechtmässigen Personendatenbearbeitung nach Art. 4 DSG (Art. 6 nDSG) nicht vereinbart werden. Da die USA den betroffenen Personen in der Schweiz keinen vergleichbaren Schutz wie diesen aus den erwähnten Bestimmungen garantieren kann, gelangt der EDÖB zum Schluss, dass auch die US-Unternehmen, welche unter dem Privacy Shield zertifiziert sind, das Niveau des angemessenen Datenschutzes nicht erreichen.[161]

Nach der Stellungnahme des EDÖB erscheint also eine sehr ähnliche Konstellation wie in der EU.[162] Das Schutzniveau des Privacy Shields zwischen der Schweiz und der USA für Datenbekanntgaben von der Schweiz in die USA ist nicht mehr geeignet das Datenschutzniveau der Schweiz zu erfüllen. In Anbetracht der Standardvertragsklauseln, gilt auch in der Schweiz, deren grundsätzliche Zulässigkeit, jedoch muss in jedem Einzelfall geprüft werden, ob das Datenschutzniveau der USA in der vorliegenden Situation als angemessen qualifiziert werden kann.[163]

Konkret wird durch den Wegfall des Privacy Shields die Verantwortlichkeit von den Behörden auf die Unternehmen umgesiedelt. Die Unternehmen müssen nun in jedem Einzelfall das angemessene Datenschutzniveau in den USA prüfen, was einen grossen Aufwand verursacht sowie eine Unsicherheit in der Rechtsanwendung mit sich bringt. Die Unternehmen müssen nun ihre Datenexporte in die USA und in andere Länder ohne angemessenes Schutzniveau dokumentieren, ihre bisherigen Prozesse des Datentransfers überprüfen sowie die Verantwortlichkeiten innerhalb des Unternehmens bestimmen. Ausserdem müssen sie ihre angewendeten Standardvertragsklauseln evaluieren, so dass der Inhalt mit den neusten Vorgaben übereinstimmt.[164] Allenfalls müssen sie auch Klauseln ergänzen, wobei diese aufgrund der derogatorischen Kraft des öffentlichen Rechts nur beschränkt wirksam sind. Zudem müssen die Unternehmen überprüfen, ob der Datenempfänger aus dem Ausland «berechtigt und in der Lage ist, die zur Durchsetzung der schweizerischen Datenschutzgrundsätze nötige Mitwirkung zu leisten.»[165] Dieser Punkt

[161] EDÖB, Stellungnahme, S. 5.
[162] WEBER, Datenexport in die USA, S. 26.
[163] WEBER/HENSELER, S. 615.
[164] WEBER, Datenexport in die USA, S. 27.
[165] EDÖB, Stellungnahme, S. 7.

wird bei den Schweizer Unternehmen zu einem signifikanten Aufwand führen und viele Unsicherheiten hervorrufen. Zudem werden die Unternehmen wohl zusätzliche technische Massnahmen zur Verhinderung des Datenzugriffs ausländischer Behörden auf die gelieferten Daten ergreifen müssen.[166] Der EDÖB erwähnt hierzu ausdrücklich eine Verschlüsselung nach den Prinzipien BYOK (bring your own key),[167] bei welchem der Kunde den Entschlüsselungsschlüssel in der Cloud verwaltet,[168] und BYOE (bring your own encryption),[169] so dass es dem Cloudanbieter nicht möglich ist, die Daten selbst zu entschlüsseln.[170] Diese technischen Massnahmen sind von besonderer Bedeutung bei Cloud Outsourcing mit externen Dienstleistern in den USA.[171]

3.2 Verhältnis US-Cloud Act mit dem Schweizer Recht

Um die Vereinbarkeit des US-Cloud Acts mit dem Schweizerischen Recht zu überprüfen, ist das heute geltende DSG, die VDSG[172] sowie die Bestimmungen des neuen DSG massgebend[173]. In der Schweiz ist es Privaten generell erlaubt, Daten zu bearbeiten, sofern die Datenbearbeitung nicht persönlichkeitsverletzend ist. Eine Persönlichkeitsverletzung liegt vor, wenn die Datenbearbeitung gegen die allgemeinen Grundsätze der Rechtsmässigkeit, Verhältnismässigkeit, Zweckgebundenheit, Erkennbarkeit und Treu und Glauben verstösst (Art. 4 DSG/Art. 6 nDSG), den Anforderungen der Datenrichtigkeit (Art. 5 DSG/Art. 6 Abs. 5 nDSG) oder diesen der Datensicherheit (Art. 7 DSG/Art. 8 nDSG) nicht genügt. Zudem müssen bei der Datenbekanntgabe ins Ausland zusätzliche Anforderungen gemäss Art. 6 DSG (Art. 16 f. nDSG) erfüllt sein. Darunter fallen beispielsweise eine zusätzliche vertragliche Schutzklausel nach lit. a, die Einwilligung der betroffenen Person gemäss lit. b oder die allgemeine Zugänglichkeit der Daten durch die betroffene Person, welche sie nicht ausdrücklich untersagt hat nach lit. f.

Die Komptabilität des US-Cloud Acts und der datenschutzrechtlichen Grundsätze scheint bedenklich. So kann beispielsweise eine Datenbearbeitung, basierend auf einer Herausgabeanordnung als Verstoss gegen Treu und Glauben angesehen werden. Dies aus dem Grund, dass die Datenbearbeitung nicht transparent ist und deshalb die

---

166 WEBER, Datenexport in die USA, S. 27.
167 Sicherheitskonzept, bei welchem nur der Kunde über den Schlüssel verfügt.
168 ROSENTHAL, S. 466.
169 Sicherheitskonzept, bei welchem der Kunde über Algorithmen zur Verschlüsselung verfügt.
170 EDÖB, Stellungnahme, S. 7.
171 WEBER, Datenexport in die USA, S. 27.
172 Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993, SR 235.11.
173 BJ, Bericht zum US-Cloud Act, S. 29.

datenschutzrechtlichen Garantien unvollständig umgesetzt wurden.[174] Auch bei heimlichen Datenbearbeitungen oder solchen mit denen die betroffene Person nicht rechnen muss, kann eine Verletzung von Treu und Glauben vorliegen.[175] Wird vor der Herausgabeandrohung eine gerichtliche Überprüfung durchgeführt, so wird die Datenbearbeitung wohl verhältnismässig sein. Da jedoch bei anderen Formen von Anfragen kein derartiger Kontrollmechanismus besteht, wird die Verhältnismässigkeitsprüfung in diesen Fällen problematisch ausfallen. Bezüglich der Notwendigkeit stellt sich die Frage, ob die klassische Rechtshilfe nicht die gleichen Erträge wirft und damit ein milderes Mittel besteht.[176]

Werden Daten unter dem Cloud Act mittels Sicherungs- und Herausgabeanordnung gespeichert oder an die US-Behörden weitergegeben, so stellt dies eine Zweckänderung dar.[177] Wie bereits ausgeführt, dürfen Personendaten nur zu einem bestimmten Zweck bearbeitet werden, welcher für die betroffene Person erkennbar ist.[178] Durch die Aufbewahrung oder das Bekanntgeben werden die Daten durch das CSP mittels eines anderen Zwecks bearbeitet als dem ursprünglichen, vertraglichen Zweck. Für eine solche Zweckänderung bedarf es einer Information an die betroffene Person sowie einen Rechtfertigungsgrund. Mögliche Rechtfertigungsgründe sind nach Art. 13 DSG (Art. 27 nDSG) die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine Datenbearbeitung welche durch das Gesetz gerechtfertigt ist, durch diese Gründe gilt eine Datenbearbeitung nicht als widerrechtliche Persönlichkeitsverletzung.[179] Gemäss Rechtsprechung des Bundesgerichts ist die Rechtfertigung einer Persönlichkeitsverletzung bezogen auf eine solche Zweckänderung nur mit grosser Zurückhaltung möglich.[180]

Damit die betroffene Person in die Datenbearbeitung einwilligt, muss sie genügend informiert werden, was die spezifische Risikosituation der Auslandsbekanntgabe beinhaltet. Die Einwilligung muss freiwillig erfolgen und kann nur dann freiwillig sein, wenn der betroffenen Person eine andere Handlungsmöglichkeit vorliegt, welche keine unzumutbaren Nachteile beinhaltet.[181] Die fehlende Verbindung zwischen der notwendigen

[174] BJ, Bericht zum US-Cloud Act, S. 30.
[175] BBl 1988, S. 449.
[176] BJ, Bericht zum US Cloud Act, S. 30 f.
[177] BJ, Bericht zum US-Cloud Act, S. 31.
[178] Vgl Kapitel 2.1.4.
[179] BJ, Bericht zum US-Cloud Act, S. 31 f.
[180] BGE 136 II 508, E. 5.2.4.
[181] RAMPINI, BSK, Rz. 6 zu Art. 13 DSG.

Datenbearbeitung der CSP aufgrund ihrer Dienstleistungen und einer Herausgabeanordnung erscheint als problematisch. Der Kunde müsste dem nicht notwendigen Zweck der Datenbekanntgabe ins Ausland zustimmen, um die Dienstleistungen vom CSP in Anspruch nehmen zu können. Werden Daten im Zusammenhang mit der Strafverfolgung und -vollstreckung bearbeitet, kann prinzipiell angenommen werden, dass keine echte Wahlfreiheit zur Einwilligung bestanden hat. Dies impliziert, dass CSP sich nicht auf die Einwilligung der betroffenen Person als Rechtfertigungsgrund für die Datenbearbeitungen und -bekanntgaben berufen können, da sich der US-Cloud Act auf das Strafverfahren bezieht.[182]

Werden Personendaten ins Ausland bekanntgegeben, so unterstehen sie nicht mehr dem schweizerischen Datenschutzrecht, sondern der ausländischen Rechtsordnung. Dadurch erhöht sich das Risiko der Persönlichkeitsverletzung. Art. 6 DSG (Art. 16 und 17 nDSG) stellt einige Voraussetzungen für eine Datenbekanntgabe ins Ausland, bei welcher die Persönlichkeit der betroffenen Person schwerwiegend verletzt werden kann. Davon kann grundsätzlich ausgegangen werden, wenn der betroffene Staat keine Gesetzgebung hat, welche ein mit der Schweiz vergleichbaren Schutz gewährleistet und deshalb kein angemessenes Datenschutzniveau hat.[183] Die USA verfügt über kein angemessenes Datenschutzniveau.[184]

Wie bereits erwähnt ist der US-Cloud Act mit seinen Herausgabeanordnungen im Anbetracht auf die datenschutzrechtlichen Grundsätzen heikel, daher kann von der Rechtswidrigkeit der Herausgabeanordnung ausgegangen werden. Folglich erübrigt sich auch eine detaillierte Analyse der Vereinbarkeit des US-Cloud Acts in Bezug auf die Datenbekanntgabe ins Ausland. Jedoch können Datenbekanntgaben ins Ausland auch bei Fehlen eines angemessenen Schutzniveau ausnahmsweise erlaubt sein, wenn es sich dabei um Tatsachen des Katalogs aus Art. 6 Abs. 2 DSG[185] handelt. In Ausnahmefällen könnte ein CSP Personendaten an US-Strafverfolgungsbehörden bekannt geben, wenn damit lebenswichtige Interessen der betroffenen Person tangiert sind oder dies für die Durchsetzung von Rechtsansprüchen laufender Strafverfahren notwendig ist. Die berührten Interessen müssen gegeneinander abgewogen werden. Bei einer schwerwiegenden Bedrohung der Persönlichkeitsrechte der betroffenen Person, von welcher grundsätzlich ausgegangen

[182] BJ, Bericht zum US Cloud Act, S. 32.
[183] BJ, Bericht zum US Cloud Act, S. 33 f.
[184] EDÖB, Stellungnahme, S. 5.; Vgl. Kapitel 3.1.4.
[185] Vgl. Kapitel 3.1.4.

werden kann, da die Personendaten an US-Behörden weitergegeben werden, sollten diese Ausnahmefälle jedoch mit Vorsicht als Rechtfertigungsgrund für eine solche Datenbekanntgabe angewendet werden.

Auch im Zusammenhang mit dem Grundrecht des Schutzes auf Privatsphäre aus Art. 13 BV und dem Grundrecht auf Achtung des Privatlebens nach Art. 8 EMRK ist eine solche Datenbearbeitung heikel.[186] Jeder Eingriff in das Privatleben muss gesetzlich vorgesehen, einen rechtmässigen Zweck anstreben und sich auf das in einer demokratischen Gesellschaft Erforderliche beschränken.[187] Auch mit diesem Hintergrund ist die Bekanntgabe von Personendaten an die US-Behörden problematisch[188], da der US Cloud Act unterschiedliche Regelungen hat betreffend Daten von US-Personen und anderen Personen, Überwachung in Echtzeit von Kommunikationsinhalten, fehlende Unterscheidung zwischen Verantwortlichen und Auftragsbearbeiter, fehlende Auskunfts- und Informationsrechte sowie fehlende Rechtsbehelfe für die betroffene Person.[189] Der fehlende Anspruch auf gerichtliche Beurteilung ist sowohl mit dem schweizerischen Datenschutzrecht unvereinbar wie auch mit der Bundesverfassung im Sinne der Rechtsweggarantie nach Art. 29a BV, welche statuiert, dass jede Person Anspruch auf eine Beurteilung durch eine richterliche Behörde hat.[190]

3.2.1 Überblick strafrechtlicher Vorschriften zum Unternehmensgeheimnis und wirtschaftlichen Nachrichtendienst

Gemäss Art. 273 des Strafgesetzbuchs (StGB)[191] wird wegen wirtschaftlichen Nachrichtendiensts mit Freiheitsstrafe verurteilt, «wer ein Fabrikations- oder Geschäftsgeheimnis auskundschaftet, um es einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich zu machen» oder wer diesen Stellen ein solches Geheimnis «zugänglich macht». Art. 273 StGB kommt aus der Kriegszustandsverordnung von 1914 hervor, in welcher sich ein generell gehaltener Tatbestand befand, nach welchem sich Personen, die auf dem Gebiet der Schweiz Nachrichtendienst zugunsten einer fremden Macht ausübten, strafbar machten. Nach 1930 wurde es aufgrund der Vorkommnisse in Italien und Deutschland notwendig, einen neuen,

[186] BJ, Bericht zum US-Cloud Act, S. 34.
[187] EGMR vom 1. Juli 2008, Liberty und andere gegen Vereinigtes Königreich, Nr. 58243/00, § 58.
[188] BJ, Bericht zum US-Cloud Act, S. 26.
[189] Vgl. Kapitel 3.1.
[190] BJ, Bericht zum US-Cloud Act, S. 35.
[191] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.

verschärfteren und optimierten Schutz gegen die Spionage aufzustellen. Mittels Bundesbeschluss vom 21. Juni 1935 wurde das sogenannte Spitzelgesetz[192] geschaffen und der Tatbestand des wirtschaftlichen Nachrichtendiensts aufgenommen.[193]

Welches Rechtsgut mittels des wirtschaftlichen Nachrichtendienstes geschützt wird ist eher schwierig zu definieren. Gemäss Bundesgericht soll Art. 273 StGB Delikte gegen den Staat sanktionieren, denn: «Der Staat hat ein Interesse daran, dass die unter seiner Gebietshoheit stehenden Personen gegen den Verrat von wirtschaftlichen Belangen geschützt seien. Wer einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder deren Agenten ein Fabrikations- oder Geschäftsgeheimnis preisgibt, beeinträchtigt schon dadurch die Interessen der nationalen Volkswirtschaft, denn jeder schweizerische Geschäftsbetrieb bildet einen Teil der gesamten schweizerischen Wirtschaft. Art. 273 setzt nicht eine unmittelbare Verletzung oder Gefährdung der staatlichen Interessen voraus. Denn in jedem wirtschaftlichen Nachrichtendienst zum Nachteil eines in der Schweiz ansässigen Unternehmens zu Gunsten des Auslandes liegt notwendigerweise eine mittelbare Verletzung oder Gefährdung der staatlichen Interessen, was zur Erfüllung des Tatbestandes von Art. 273 genügt».[194] Der wirtschaftliche Nachrichtendienst soll folglich «den Schutz der Gebietshoheit und die Abwehr der Spitzeltätigkeit zur Erhaltung der nationalen Wirtschaft» bezwecken.[195]

Das Fabrikations- oder Geschäftsgeheimnis stellt das Angriffsobjekt von Art. 273 StGB dar. Dabei muss der Begriff des Geheimnisses grosszügig ausgelegt werden[196], denn auch fragmentarische Informationen über einen geheimen Fabrikations- oder Geschäftsprozess fallen darunter.[197] Unter Fabrikationsvorgänge und die Geschäftstätigkeit fallen alle Angaben über die Beschaffung und Bearbeitung von Material, technisches Wissen sowie jegliche Aspekte über kommerzielle Tatsachen, wie beispielsweise Kundendaten, Daten über die Buchhaltung und markt-, personal- oder preispolitische Daten.[198] Fundamental ist es, dass das Geheimnis in einer Verbindung zur Schweiz steht, auch wenn die tatbestandsmässigen Handlungen vollständig im Ausland verwirklicht wurden.[199] Das schutzwürdige Interesse am Geheimnis ist eine selbstständige Voraussetzung des

[192] Spitzelgesetz, Bundesbeschluss vom 21. Juni 1935.
[193] GERMANN, S. 12 f.
[194] BGE 101 IV 312, E. 1.
[195] BGE 108 IV 41, E. 3.
[196] TRECHSEL/VEST, PK StGB, Rz. 3 zu Art. 273 StGB.
[197] OGer BL, Urteil vom 23.11.1993, BJM 1995, 31 ff., E. 5.
[198] BAZZI, Rz. 111 ff.
[199] BGE 141 IV 155, E. 4.1.

Geheimnisbegriffs.[200] Es wird zudem vorausgesetzt, dass der verfügungsberechtigte über die Tatsache, diese auch geheim halten will, folglich dass ein Geheimhaltungswille besteht[201] und dieser erkennbar ist.[202]

Bei Datenbekanntgaben ins Ausland ist die Frage nach dem Geheimhaltungswillen von grosser Bedeutung.[203] Aus datenschutzrechtlicher Sicht wäre ein Ausschluss des Geheimhaltungswillens, unter gewissen erfüllten Voraussetzungen, zu begrüssen. Diese wären erfüllt wenn; (1) die Bekanntgabe für die Zwecke und im Rahmen einer Aktivität erfolgt, welche die betroffenen Dritten aufgrund der Umstände typischerweise annehmen müssen und die nach der allgemeinen Lebenserfahrung geduldet werden müssen, (2) die Bekanntgabe verhältnismässig und zweckmässig ist, (3) die Datenempfänger damit nicht mehr machen, als das was das Unternehmen, welchem die Daten anvertraut wurden, selbst tun dürfte, (4) die Empfänger die Daten mit angemessenen technischen und organisatorischen Massnahmen vor einer unbefugten Bearbeitung schützen.[204]

Der Ausschluss des Geheimhaltungswillen entspricht der Erwartungshaltung der heutigen Wirtschaftswelt der Schweiz,[205] jedoch kann diese Erwartungshaltung nicht den Ausschluss des erkennbaren Geheimhaltungswillen zur Folge haben.[206] Art. 273 StGB setzt keine tatsächliche Gefährdung oder Verletzung der schweizerischen Wirtschaftsinteressen voraus.[207] Die Norm soll den rechtlichen Schutz vor Eingriffen in den Geheimbereich gewährleisten, womit insbesondere der Schutz vor «rechtswidrigem Kenntnis verschaffen» angestrebt wird.[208]

3.2.2 Konkrete Anwendungsvorschriften

Mit Hinblick auf die Nutzung von Clouds stellt sich die Frage ob Schweizer Unternehmen Art. 273 StGB verletzen, indem sie Daten in US-Clouds abspeichern. Man kann davon ausgehen, dass Unternehmen auch Geschäftsgeheimnisse in der Cloud abspeichern, dieser Begriff ist wie bereits ausgeführt weit auszulegen. Sind diese Clouds in einem Land ohne angemessenes Schutzniveau, wie in den USA, und können dadurch ausländische

[200] BGE 141 IV 155, E. 4.2.1.
[201] HUSMANN, BSK, Rz. 24 zu Art. 273 StGB.
[202] BAZZI, Rz. 175.
[203] HUSMANN, BSK, Rz. 36 zu Art. 273 StGB.
[204] ROSENTHAL, Rz. 24 zu Art. 273 StGB.
[205] ROSENTHAL, Rz. 25 zu Art. 273 StGB.
[206] HUSMANN, BSK, Rz. 36 zu Art. 273 StGB.
[207] BGE 98 IV 209, E. 1b.
[208] HUSMANN, BSK, Rz. 42 zu Art. 273 StGB; LIVSCHITZ, § 18 Rz. 18.107 f.

Behörden auf diese Daten zugreifen, wie die NSA, so kann man argumentieren, dass diese Handlung unter den Tatbestand von Art. 273 StGB fällt. In diesem Sinne macht das Schweizer Unternehmen ihre Geschäftsgeheimnisse einer fremden amtlichen Stelle, wie dem US-Nachrichtendienst, zugänglich. Man könnte einen Vorsatz zur Zugänglichkeit der Geheimnisse begründen, denn die US-Behörden können auf die Clouddaten zugreifen und die Unternehmen speichern ihre Daten dennoch darauf ab. Nach der hier vertretenen Auffassung geht es jedoch zu weit, diesen Unternehmen abfälliger wirtschaftlicher Nachrichtendienst vorzuwerfen. Denn obwohl sie ohne Zweifel Geschäftsgeheimnisse auf Clouds abspeichern, erscheint nicht schlüssig, dass dies ein «zugänglich machen» sei. Hier wird vertreten, dass es sich erst um ein «zugänglich machen» handeln würde, wenn die US-Behörden bereits ohne spezifischen Grund auf jede Cloud zugreifen würde oder das Unternehmen zielgerichtet Geheimnisse in der Cloud speichert, um die US-Behörden aktiv über diese zu informieren. Solange sie die Clouds jedoch als Ablageort für ihre Daten nutzen und die US-Behörden nicht prinzipiell auf alle Daten in Clouds zugreifen, handelt es sich nicht um Handlungen die unter den Straftatbestand des wirtschaftlichen Nachrichtendienstes nach Art. 273 StGB fallen würden.

3.3 Aktuelle Entwicklung zur Übertragung von Personendaten in Drittländer

Am 22. Dezember 2021 hat die Datenschutzbehörde Österreich (DSB) einen ausführlichen Teilentscheid gefällt basierend auf einer Beschwerde von NOYB des NGO von Maximilian Schrems gegen einen Verlag und gegen Google LLC in den USA. NOYB brachte vor, dass der Einsatz von Google Analytics auf der Website des Verlags die DSGVO verletzte. Dies, da mittels Google Analytics Personendaten an Google in den USA bekanntgegeben werden, ohne dass dafür die Voraussetzungen von Art. 44 ff. DSGVO über die Bekanntgabe von Personendaten in Drittstaaten erfüllt waren.[209] Google Analytics ist ein Webanalyse-Tool mit welchem die Trafficeigenschaften der Kunden von Google gemessen wird. Dazu gehört unter anderem die Messung des Traffics von Besuchern einer Website, deren Verhalten und wie sie mit der Website interagieren. Ein Website-Betreiber kann ein Google-Analytics Konto erstellen und erhält dann Berichte über

[209] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257.

seine Website. Damit kann er die Wirksamkeit seiner Werbekampagnen messen und optimieren.[210]

Als Folge zur Google Analytics Implementierung des Verlags auf deren Website wurden Informationen des Websitebesuchers an die Server von Google übermittelt. Bei diesen Daten handelt es sich unter anderem um einzigartige Online-Kennungen («unique identifier»), welche die Geräte vom Websitebesucher und -besitzer identifizieren, Adressen, die der Websitebesucher besucht hat, Informationen über Browser, Bildschirmauflösung, Sprachauswahl, Betriebssystem wie auch Datum und Uhrzeit des Besuchs und die IP-Adresse des Geräts des Besuchers. Es stellte sich die Frage, ob es sich bei diesen Angaben um personenbezogene Daten nach Art. 4 DSGVO[211] handelt.[212] Gemäss DSB reicht es aus, wenn Massnahmen ergriffen werden, wie in casu die Zuordnung von Kennzahlen, um Website-Besucher zu individualisieren.[213] Durch die Kombination der Kennnummern mit weiteren Elementen wie die oben angegebenen Informationen, ist die Identifizierung des Websitebesuchers noch realisierbarer. Die DSB kommt daher zum Schluss, dass es sich bei den ausgeführten Informationen um personenbezogene Daten handelt.[214]

Zudem setzte sich das DSB mit der Frage auseinander, ob personenbezogenen Daten unter Achtung von Art. 44 ff. DSGVO in die USA übermittelt wurden. Um das angemessen Schutzniveau aus Art. 44 DSGVO zu erfüllen, gibt es drei Möglichkeiten: der Angemessenheitsbeschluss nach Art. 45 DSGVO, die geeigneten Garantien nach Art. 46 DSGVO und die Ausnahmen für bestimmte Fälle nach Art. 49 DSGVO.[215] Der EU-US Angemessenheitsbeschluss ist ungültig, demnach kann die Datenübermittlung nicht nach Art. 45 DSGVO abgehandelt werden. Der Verlag und Google LLC haben Standarddatenschutzklauseln gemäss Art. 36 Abs. 2 lit. c DSGVO für die Übermittlung personenbezogener Daten abgeschlossen. Diese sind gemäss EuGH-Urteil Schrems II grundsätzlich nicht zu bemängeln, jedoch sind sie bloss ein Vertrag und dadurch kein effektives Schutzmittel, wenn das Recht des Drittlands ihren Behörden den Zugriff auf die Daten gewährleistet. Da die USA kein angemessenes Schutzniveau gewährleistet[216] und Google LLC als CSP

[210] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. C.3.
[211] Vgl. Kapitel 2.2.3.
[212] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.2. 2.a.
[213] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.2. 2.b.
[214] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.2. 2.c.
[215] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.3. 2.b.
[216] Vgl. Kapitel 3.1.3.

im Sinnen von 50 U.S. Code § 18881(b)4)[217] zu qualifizieren ist, untersteht sie der Überwachung durch die US-Nachrichtendienste gemäss FISA 702[218].

Google LLC ist demzufolge verpflichtet den US-Behörden personenbezogene Daten zur Verfügung zu stellen. Das DSB kommt zum Schluss, dass die Datenübermittlung nicht bloss auf die Standarddatenschutzklausen gestützt werden kann.[219] Die geeigneten zusätzlichen Massnahmen können vertraglicher, technischer oder organisatorischer Art sein[220] und sollten die Rechtsschutzlücken, also die vorhandenen Überwachungs- und Zugriffsmöglichkeiten des US-Nachrichtendienstes, schliessen. Google LLC hat zwar zusätzliche Massnahmen[221] eingeführt, jedoch ist bei diesen Massnahmen nicht erkennbar inwiefern sie effektiv sein sollten im Sinne des Schrems II Urteils. Google LLC führte zwar aus, dass die Daten von Google Analytics personenbezogene Daten sind, jedoch seien sie pseudonym.[222] Gemäss der Deutschen Datenschutzkonferenz (DSK) werden Kennungen dazu genutzt die Individuen adressierbar und differenzierbar zu machen, anstatt die identifizierenden Daten zu verstecken oder zu löschen, wie dies bei der Pseudenomysierung eigentlich der Fall sein sollte.[223] Die DSB beurteilte das Tool Google Analytics als unvereinbar mit Art. 44 ff. DSGVO.[224]

3.3.1 Aktuelle Entwicklungen zur Übertragung von Personendaten mittels Clouds

Bei der Verarbeitung von Daten durch CSP muss nebst der Rechtmässigkeitsprüfung nach Art. 6 Abs. 1 DSGVO, wobei für die CSP nur die Einwilligung (lit. a), vertragliche Verpflichtung (lit. b) oder die überwiegenden berechtigten Interessen (lit. f) in Frage kommen[225], zudem überprüft werden, ob es zu einer Übermittlung personenbezogener Daten an ein Drittland kommt. Bei Inhalten, welche durch grosse Drittanbieter zur Verfügung gestellt werden, ist dies häufig der Fall. Das kann ein Problem darstellen, wenn diese Länder kein Angemessenheitsbeschluss mit der EU-Kommission haben, wie beispielsweise die USA. Werden personenbezogene Daten im Zusammenhang mit der anhaltenden Nachverfolgung von Nutzerverhalten in Apps oder auf Webseiten verarbeitet,

---

[217] 50 U.S. Code § 1881(b)4.
[218] 50 U.S. Code § 1881a.
[219] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.3. 2.b.
[220] EDPB, Empfehlungen 01/2020, Rz. 51.
[221] Vgl. Kapitel 4.1.2.
[222] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.3. 2.b.
[223] DSK, 2019, S. 15.
[224] DSB vom 22.12.2021, GZ: D155.027, 2021-0.586.257, E. D.5.
[225] DSK, 2021, S. 27.

können sie prinzipiell nicht mittels Einwilligung nach Art. 49 Abs. 1 lit. a DSGVO in ein Drittland übermittelt werden.[226]

Auch die französische Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat die Verwendung von Google Analytics mit ihrem Entscheid vom 10. Februar 2022 als unrechtmässig beurteilt. Auch dieser Entscheid basiert auf einer Beschwerde von NOYB. Die CNIL beurteilt die zusätzlichen Massnahmen von Google LLC als unzureichend, weshalb ein Risiko für betroffenen Personen besteht. Es fehlt an den für die Datenermittlung geeigneten Garantien. Die Übertragung von Personendaten in die USA mittels Kennung, was wie bereits ausgeführt ein personenbezogenes Datum darstellt, ist unrechtmässig.[227]

Die Tendenz des europäischen Rechtgebiets geht klar gegen eine Datenübermittlung in die USA. Diese Sicherheitsbedenken bezüglich der Weitergabe von personenbezogenen Daten an die US-Behörden werden nun angegangen wie es bereits in Österreich und Frankreich zu sehen ist. Zudem sind auch in Deutschland zahlreiche Beschwerden über Google Analytics eingegangen, wie an der Herbstkonferenz des Berufsverbands der Datenschutzbeauftragten Deutschlands[228] von einer Referatsleiterin im Bayerischen Landesamt für Datenschutzaufsicht berichtet wurde betrifft es 200'000 Fälle. Somit wird sich auch die deutsche Aufsichtsbehörde mit der Google Analytics Thematik befassen müssen.

Es stellt sich nun die Frage, inwiefern die Problematik von Google Analytics auch bei Clouds besteht. Weiter steht zur Diskussion was der Unterschied zwischen Datenübermittlungen in die USA von Google LLC über Google Analytics gegenüber der Nutzung von Clouds in den USA ist. Speichert man seine Daten in einer Cloud beispielsweise von Microsoft, welche ihr Datenzentrum in den USA haben, so können die US-Behörden auch auf diese Daten zugreifen. In beiden Konstellationen werden personenbezogene Daten in ein Drittland übermittelt, welches einen ungenügendes Schutzniveau hat, wie in diesem Beispiel die USA. Nach der hier vertretenen Auffassung besteht kein Unterschied mit Hinblick auf die Hauptproblematik, den Datentransfer in die USA. Sollte es in Zukunft zu einem Fall kommen, der die Cloud Thematik behandelt, so müssten die Gerichte ihrem

[226] DSK, 2021, S. 31 f.
[227] CNIL S. 1 ff.
[228] https://www.bvdnet.de/herbstkonferenz-datenschutz/.

jetzigen Ansatz folgen und auch Clouds als unvereinbar mit der DSGVO bzw. der DSG einstufen.

4 Standardvertragsklauseln

4.1 Überblick der Standardvertragsklauseln

Wie bereits ausgeführt, dürfen personenbezogene Daten beziehungsweise Personendaten nicht in Länder ohne angemessenes Datenschutzniveau übermittelt werden. Es ist jedoch unter Umständen möglich Daten in ein solches Land zu transferieren, wenn ein angemessener Schutz auf eine andere Art und Weise gewährleistet werden kann, wie zum Beispiel mittels Vertrags. Bei solchen Verträgen werden Standardvertragsklauseln (SCC) als ein Instrument für eine vertragliche Absicherung des angemessenen Datenschutzniveaus genutzt.[229]

4.1.1 Historie der Standardvertragsklauseln

Die europäische Kommission kann SCC erlassen, welche mittels Prüfverfahren nach Art. 93 Abs. 2 DSGVO i.V.m. Art. 5 der EU-Verordnung Nr. 182/2011[230] entstehen müssen, damit gewährleistet ist, dass diese SCC die geeigneten Garantien liefern.[231] Bis vor kurzer Zeit gab es die folgenden drei SCC welche durch die europäische Kommission statuiert wurden[232]:

- Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer[233]

- Alternative Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer[234]

[229] EDÖB, Standardvertragsklauseln und Musterverträge, S. 2.
[230] Verordnung (EU) Nr. 182/2011 des europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedsstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ABl. EU vom 28. Februar 2011, Nr. L 55/13.
[231] LANGE, Rz. 25 zu Art. 46 DSGVO.
[232] LANGE, Rz. 34 zu Art. 46 DSGVO.
[233] Entscheidung der Kommission 2001/497/EG vom 15. Juni 2001, ABl. EU vom 4. Juli 2001, Nr. L 181/19.
[234] Entscheidung der Kommission 2004/915/EG vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl. EU vom 29. Dezember 2004, Nr. L 385/74.

– Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern[235]

Mit den SCC I vom 15. Juni 2001 und den SCC II vom 17. Dezember 2004 wurde der Datentransfer zwischen zwei Verantwortlichen geregelt, diese SCCs sind grösstenteils gleichartig. Sie unterscheiden sich jedoch in der Haftung, indem Klausel 6 der SCC I die Parteien zu einer Solidarhaftung verpflichtet gegenüber der betroffenen Person mit Regressmöglichkeit im Innenverhältnis. Eine Haftung für punitive damages, also Entschädigungen mit Strafcharakter geprägt vom amerikanischen Recht, ist nicht explizit ausgeschlossen. In den SCC II hingegen werden punitive damages ausdrücklich ausgeschlossen und die betroffene Person kann die Parteien nur für Rechtsverletzungen haftbar machen.[236] Trotz ihrer Ähnlichkeit dürfen die Klauseln der beiden Musterverträge gemäss Art. 1 der Entscheidung 2001/497/EG nicht kombiniert oder abgeändert werden. Diese beiden SCC bedürfen nach Art. 46 Abs. 2 DSGVO keiner Genehmigung, jedoch gelten sie nicht für die Übermittlung personenbezogener Daten an einen Auftragsverarbeiter in einem Drittland. Dafür werden die SCC für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern benötigt.[237]

Seit Februar 2010 gibt es diese SCC für die Übermittlungen durch Auftragsverarbeiter. Ebendiese SCC waren anwendbar für den Datentransfer durch Verantwortliche an Auftragsverarbeiter, während die SCC I und II bei Übermittlungen durch Verantwortliche an Empfänger, welche die Daten ihrerseits zu eigenen Zwecken erhalten und als Verantwortliche agieren, zu verwenden waren.[238] Auftragsverarbeiter kann eine natürliche oder juristische Person sein, welche gemäss Art. 4 Ziff. 8 DSGVO «personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet». Er tätigt den tatsächlichen Verabeitungsprozess, aber entscheidet nicht selbst darüber mit welchen Mitteln und zu welchem Zweck die Daten verarbeitet werden. Er handelt ausschliesslich auf Anweisung des Verantwortlichen, welcher auch für die Handlungen des Auftragverarbeiters aufkommen muss.[239]

---

[235] Beschluss der Kommission 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. EU vom 12. Februar 2010, Nr. L 39/5.

[236] THÜSING/FORST, § 17 Rz. 24.

[237] THÜSING/FORST, § 17 Rz. 22.

[238] LANGE, Rz. 35 zu Art. 46 DSGVO.

[239] MARTINI, Rz. 2 zu Art. 28 DSGVO.

Der Verantwortliche ist diejenige natürliche oder juristische Person, welche allein oder mit anderen über die Zwecke und Mittel der Datenverarbeitung bestimmt.[240]

Nachdem das Privacy-Shield durch den EuGH mittels Schrems II Urteil als ungültig erklärt wurde,[241] veröffentlichte die EU-Kommission am 12. November 2020 einen Entwurf der neuen SCC und startete die Konsultationsphase, welche bis am 10. Dezember 2020 andauerte.[242] Im Juni 2021 hat die Kommission mittels Durchführungsbeschluss[243] die neuen SCC für die Übermittlung personenbezogener Daten an Drittländer erschaffen. Damit bietet die Kommission i.S.v. Art. 46 Abs. 2 lit. c DSGVO vier unterschiedliche Module von SCC an, welche die vier Arten von Datenübermittlung abdecken sollen. Bei diesen vier Typen handelt es sich um; Übermittlung vom Verantwortlichen an Verantwortliche (Controller to Controller, Modul 1), Übermittlung von Verantwortlichen an Auftragsverarbeiter (Controller to Processor, Modul 2), Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter (Processor to Processor, Modul 3) und Übermittlung von Auftragsverarbeitern an Verantwortliche (Processor to Controller, Modul 4). Wer diese SCC nutzen will, muss das passende Modul für die Umstände des Datenexporteurs und -importeurs auswählen.[244]

Wie bis anhin finden die neuen SCC gemäss Art. 1 Abs. 1 Durchführungsbeschluss 2021/914 (nachfolgend «neuer SCC-Beschluss») Anwendung auf Datenübermittlungen zwischen einem Datenexporteur der EU und einem Datenimporteur in einem Drittland. Jedoch darf der aussereuropäische Datenimporteur nicht bereits in den Anwendungsbereich von Art. 3 Abs. 2 DSGVO fallen.[245] Durch diese Bestimmung soll wohl garantiert werden, dass der Datenimporteur im Drittland vertraglich der DSGVO untersteht, jedoch scheint es nicht notwendig zu sein dies vertraglich mittels SCC zu vereinbaren, wenn die Übermittlung ohnehin unter die Anwendung der DSGVO fällt. Ist es für den Datenexporteur mühsam zu ermitteln, ob der Datenimporteur die Voraussetzungen von Art. 3 Abs. 2 DSGVO erfüllt, ist der Abschluss eines SCC zu empfehlen.[246]

---

240 ERNST, Rz. 55 zu Art. 4 DSGVO.
241 Vgl. Kapitel 3.1.3.
242 Draft of Commission implementing Decision, standard contractual clauses.
243 Durchführungsbeschluss der Kommission 2021/914 vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. EU vom 7. Juni 2021, Nr. L 199/31.
244 LANGE, Rz. 36 zu Art. 46 DSGVO.
245 Vgl. Kapitel 2.2.2.
246 BAUMGARTNER/HANSCH/ROTH, S. 610.

Die neuen SCC traten gemäss Art. 4 Abs. 1 neuer SCC-Beschluss am 27. Juni 2021 in Kraft und die alten SCC wurden gemäss Art. 4 Abs. 2 und Abs. 3 neuer SCC-Beschluss per 27. September 2021 aufgehoben. Bestehende Verträge mit den alten SCC unterstehen einer Umstellungsfrist bis zum 27. Dezember 2022, jedoch nur wenn die Verarbeitungsvorgänge unverändert bleiben und gewährleistet werden kann, dass mit den bisherigen SCC die geeigneten Garantien nach Art. 46 Abs. 1 DSGVO eingehalten werden. Das bedeutet, dass die SCC um zusätzliche vertragliche Massnahmen ergänzt werden müssen, um den Aufforderungen des Schrems II Urteils[247] nachzukommen.[248]

4.1.2 Anhang Standardvertragsklausel

Die Klauseln der SCC werden durch Anlagen ergänzt, die ebenfalls ein Bestandteil des Vertrages sind und von den Parteien auf ihre Bedürfnisse angepasst werden müssen. Die neuen SCC umfassen drei Anhänge. In Anhang I müssen die Parteien für die vier Module die Liste der Parteien aufnehmen sowie eine detaillierte Beschreibung der Datenübermittlung aufführen. Dadurch werden die Art und der Zweck der Datenübermittlung bzw. der daraus folgenden Verarbeitung der Daten sowie Weiterverarbeitungen dargelegt.[249] Die Bestimmung der Kategorie der betroffenen Personen, übermittelten personenbezogenen Daten, übermittelte sensible Daten (falls vorhanden), die Übermittlungshäufigkeit und Dauer der Speicherung sind ebenfalls aufzunehmen und die zuständige Aufsichtsbehörde ist zu bestimmen.[250]

Anhang II verlangt eine Beschreibung der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Daten, die vom Datenimporteur und seinen Unterauftragsverarbeitern ergriffen werden. Dabei muss die Art, der Umfang, die Umstände und der Zweck der Verarbeitung sowie die Risiken für die Rechte und Freiheiten beschrieben werden. Auch wenn es nicht ausdrücklich erwähnt wurde, sollten die Massnahmen des Datenexporteurs zur Garantie der Datenübermittlung an den Datenimporteur wohl in diesem Anhang ebenfalls beschrieben werden.[251] In Anhang II sind einige Beispiele für mögliche Massnahmen aufgeführt, jedoch handelt es sich dabei nicht um eine abschliessende Liste. Auch zukünftige rechtliche, organisatorische oder technische

---

[247] Vgl. Kapitel 3.1.3.
[248] BAUMGARTNER/HANSCH/ROTH, S. 609.
[249] BAUMGARTNER/HANSCH/ROTH, S. 610.
[250] Durchführungsbeschluss der Kommission 2021/014 vom 4. Juni 2021, ABl. EU vom 7. Juni 2021, Nr. L 199/31, Anhang I.
[251] BAUMGARTNER/HANSCH/ROTH, S. 610.

Entwicklungen können zu neuen Massnahmen führen, die beachtet werden müssen. Bei der Auswahl der zusätzlichen Massnahmen ist darauf zu achten, dass die Massnahmen den notwendigen Schutz der Übermittlungen effektiv sicherstellen. Im Sinne des Schrems II Urteil ist eine zusätzliche Massnahme nur dann effektiv, wenn sie exakt diejenigen Rechtsschutzlücken schliesst, die der Datenexporteur festgestellt hatte, als er die Rechtsvorschriften im Drittland für seine Datenübermittlung prüfte. Kann er auch mit den zusätzlichen Massnahmen kein angemessenes Schutzniveau erreichen, so hat er die Datenübermittlung zu unterlassen.[252]

Im Falle einer Übermittlung an Cloud-Anbieter können nach dem heutigen Standard der Technik keine wirksamen technischen Massnahmen gefunden werden. Dies da es, wenn der Datenexporteur personenbezogene Daten an einen Cloud-Anbieter in einem Drittland transferiert, um die personenbezogenen Daten dort verarbeiten zu lassen und für die Datenverarbeitung der Zugriff auf unverschlüsselte Daten notwendig ist, nicht möglich ist diese Daten entweder zu pseudonymisieren oder verschlüsseln.[253] Dies da der Cloud-Anbieter bei Übermittlungen von personenbezogenen Daten an den Cloud-Anbieter Zugang auf die unverschlüsselten Daten angewiesen ist, um die ihm übergebende Aufgabe zu erfüllen. Zudem haben die Behörden des Empfängerlandes USA die Befugnis, auf ebendiese Daten zuzugreifen, dies geht über die Erforderlichkeit und Verhältnismässigkeit aus.[254] Es scheint nach dem aktuellen Stand der Technik keine wirksame technische Massnahme zu geben, die einen solchen Eingriff in die Grundrechte der betroffenen Person verhindern könnte.[255] Vorbehalten bleibt das Entstehen einer wirksamen technischen Massnahme im Laufe der Entwicklungen der Technik.

Organisatorische Massnahmen zur Gewährleistung eines angemessenen Schutzniveaus können interne Strategien, Organisationsmethoden und Standards sein, welche von den Verantwortlichen und Auftragsverarbeiter selbst angewendet werden und den Datenimporteuren in Drittländern verordnet werden können. Dies kann zum schematischen Schutz der personenbezogenen Daten im ganzen Verarbeitungszyklus führen. Durch die Anwendung solcher Massnahmen, ist die Einhaltung von EU-Recht noch nicht garantiert, jedoch können sie zu einer höheren Risikosensibilität beim Datenexporteur führen und je nach Rechtslage im Drittland sind sie erforderlich, um das Schutzniveau gleichwertig zu

[252] EDPB, Empfehlungen 01/2020, Rz. 74 f.
[253] EDPB, Empfehlungen 01/2020, Rz. 93 f.
[254] Vgl. Kapitel 2.1.4.
[255] EDPB, Empfehlungen 01/2020, Rz. 94.

halten.[256] Für Unternehmen bietet sich eine Aufstellung interner Grundsätze mit eindeutigen Zuständigkeiten für Datenübermittlungen, Arbeitsanweisungen und Berichtswegen an. Ein Team aus Experten aus Datenschutzrecht und IT für behördliche Datengesuche ist für die Unternehmen von Vorteil. Für Mitarbeitende, welche solche Ersuche bearbeiten, sind laufend angepasste Schulungsprogramm empfehlenswert, es ist massgebend, dass auch sie sensibilisiert sind.[257] Als Transparenzmassnahme sollen Unternehmen, die behördlich gestellten Zugriffsersuche und dessen Bearbeitung dokumentieren, so kann die Aufstellung dem Datenexporteur auf Verlangen ausgehändigt werden.[258] Zudem sollen Unternehmen überprüfen, ob die Übermittlung personenbezogener Daten in jedem Fall erforderlich ist oder ob man auch von der Übermittlung bestimmter Daten absehen kann. Dies würde in einer Datenminimierung resultieren, was die Gefahr unbefugter Datenzugriffe reduziert.[259] Die erwähnten Massnahmen sollten regelmässig überprüft werden, damit das angemessene Schutzniveau laufend sichergestellt werden kann.[260]

Anhang III muss für die Module zwei und drei vom Unterauftragsverarbeiter ausgefüllt werden, wenn für deren Beizug eine gesonderte Genehmigung nach Klausel 9 lit. a Option 1 Durchführungsbeschluss 2021/914 vereinbart wurde. Der Datenimporteur darf gemäss dieser Klausel keine Verarbeitungstätigkeiten, die er im Auftrag des Datenexporteurs durchführt, ohne vorherige schriftliche Genehmigung des Exporteurs an einen Unterauftragsverarbeiter vergeben. In Anhang III sind Namen, Anschrift, Kontaktperson und Verarbeitungsbeschreibung, inklusiver klarer Abgrenzung bei mehreren Unterauftragsverarbeitern anzugeben.[261]

4.2 Folgen für das Schweizer Recht

Datenübermittlungen mittels Vertrags müssen gemäss Art. 6 Abs. 3 DSG dem EDÖB gemeldet werden und gemäss Art. 16 Abs. 2 lit. d nDSG dürfen Personendaten ins Ausland bekannt gegeben werden, wenn mittels SCC ein angemessener Datenschutz garantiert werden kann, sofern das EDÖB diese vorgängig genehmigt, ausgestellt oder anerkannt hat. Nach heute geltendem Schweizer Recht unterstehen Datenexporteure gemäss Art. 24 Abs. 2 lit. a DSG einer Meldepflicht gegenüber dem EDÖB, wenn sie Daten auf

[256] EDPB, Empfehlungen 01/2020, Rz. 128.
[257] EDPB, Empfehlungen 01/2020, Rz. 130 f.
[258] EDPB, Empfehlungen 01/2020, Rz. 133.
[259] EDPB, Empfehlungen 01/2020, Rz. 137.
[260] EDPB, Empfehlungen 01/2020, Rz. 142.
[261] BAUMGARTNER/HANSCH/ROTH, S. 610.

vertraglicher Grundlage übermitteln. Werden jedoch die vom EDÖB erstellten oder anerkannten SCC verwendet, so gilt die Meldepflicht gemäss Art. 6 Abs. 3 VDSG als erfüllt, wenn das EDÖB in allgemeiner Form über die Verwendung in Kenntnis gesetzt wird.

Mit dem nDSG wird keine Meldepflicht mehr bestehen, sofern die anerkannten SCC genutzt werden. Das EDÖB hatte die alten SCC der EU für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG anerkannt, jedoch sind sie ab dem 27. September 2021 aberkannt. Am 27. August 2021 anerkannte der EDÖB die neuen SCC der EU mit dem Vorbehalt, dass sie falls erforderlich in einem konkreten Fall angepasst oder erweitert werden.[262]

Für Schweizer Datenexporteure ist es nebst der Beachtung von Art. 6 DSG über die grenzüberschreitende Bekanntgabe ebenfalls essenziell die DSGVO zu beachten, da sie aufgrund ihrer extraterritorialen Wirkung auch anwendbar sein kann.[263] Es ist wichtig zu unterscheiden, ob kein Anknüpfungspunkt zur DSGVO gegeben ist und die Datenübermittlung lediglich der DSG untersteht oder ob die Datenübermittlung aufgrund der extraterritorialen Anwendbarkeit des DSGVO in ihren Anwendungsbereich fällt und in diesen der DSG. SCC, die nur für Datenübermittlungen unter dem DSG genutzt werden, können an die DSG angepasst werden, damit der betroffenen Person keine Nachteile entstehen. Handelt es sich aber um Datenübermittlungen unter der DSGVO, so dürfen die SCC nicht abgeändert werden gemäss Klausel 2 der neuen SCC. Untersteht die Datenübermittlung der DSG wie auch der DSGVO so können die Parteien entweder zwei separate Regelungen, einerseits abgedeckt nach dem DSG und andererseits nach dem DSGVO, vereinbaren oder sie können die Datenbearbeitungen ausschliesslich der DSGVO unterstellen, dabei sind jedoch auch einige Anpassungen notwendig.[264]

Damit die SCC dem Schweizer Recht entsprechen und damit ein angemessenes Datenschutzniveau gewährleisten, sind folgende Anpassungen nötig: Die zuständige Aufsichtsbehörde soll ausschliesslich das EDÖB sein oder es soll eine parallele Aufsicht von EDÖB und EU-Behörde je nach Rechtsgebiet geben. Die Rechtswahl sollte auf Schweizer Recht fallen oder auf ein Recht eines Mitgliedstaates, dass eine Drittbegünstigung zulässt. Der Drittbegünstigte kann gemäss Klausel 3 der neuen SCC bestimmte Rechte

[262] EDÖB, Standardvertragsklauseln und Musterverträge, S. 2 f.
[263] Vgl. Kapitel 2.2.2.
[264] EDÖB, Standardvertragsklauseln und Musterverträge, S. 3.

gegenüber den Parteien direkt geltend machen und allenfalls durchsetzen. Für Streitigkeiten aus dem Vertrag können die Parteien den Gerichtsstand frei vereinbaren, handelt es sich aber um Streitigkeiten über Datenübermittlungen unter der DSGVO so muss ein Gerichtsstand in einem EU-Mitgliedsstaat vereinbart werden. Es empfiehlt sich einen alternativen Gerichtsstand in der Schweiz zu vereinbaren, falls es sich um betroffene Personen mit allgemeinem Aufenthalt in der Schweiz handelt. Sind in den SCC Verweise auf das DSGVO zu finden, so müssen sie auf das DSG angepasst werden, wenn es sich um Übermittlungen unter dem DSG handelt. Dadurch können Missverständnisse bei der Vertragsauslegung vermieden werden. Ist die DSGVO ebenfalls anwendbar so soll klar definiert werden, welche Verweise die DSGVO betreffen und welche das DSG. Bei einer ausschliesslichen Datenübermittlung unter dem DSGVO bedarf es keiner solchen Präzisierung. Bis das nDSG in Kraft trifft sind unter Schweizer Recht auch juristische Personen dem Datenschutz unterstellt.[265] Deshalb sollten die SCC bis zum Inkrafttreten der nDSG mit einem Anhang ergänzt werden, der den Schutz der juristischen Personen einschliesst, da die DSGVO auf diese nicht anwendbar ist[266].[267]

5 Praxisempfehlung

5.1 Datentransfer-Folgenabschätzung

Durch die neuen SCC ergibt sich nun auch die Pflicht aus Klausel 14 des neuen SCC-Beschluss für den Datenexporteur und -importeur, sich davon zu überzeugen, dass der Vertragspartner seinen Pflichten, welche sich aus den SCC ergeben, nachkommen kann. Diese Klausel 14 über «Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken» verlangt umfassende Massnahmen. Das Kernelement dabei ist die Datentransfer-Folgenabschätzung in Bezug auf die «geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland».[268] Auch bei der Verwendung der neuen SCC ist es erforderlich die Rechtslage im Drittland zu prüfen sowie ergänzende Massnahmen einzuhalten.[269] Das EDPB hat im Juni 2021 seine Empfehlungen für die Datentransfer-Folgenabschätzung veröffentlicht.[270] Wie bereits ausgeführt müssen die Verantwortlichen überprüfen ob das Recht und die Praxis des Drittlands die

[265] Vgl. Kapitel 2.1.2.
[266] Vgl. Kapitel 2.2.3.
[267] EDÖB, Standardvertragsklauseln und Musterverträge, S. 5 ff.
[268] CONRAD/SIARA, S. 472.
[269] DSK, Pressemitteilung.; EDPB, Empfehlungen 01/2020, Rz. 5.
[270] EDPB, Empfehlungen 01/2020.

angemessenen Schutzgarantien beeinträchtigen. Der EuGH lässt den Datenexporteuren die Möglichkeit offen zusätzliche Massnahmen zu ergreifen, um das angemessene Schutzniveau zu erreichen.[271] Die Datenexporteure müssen in jedem Fall beurteilen, ob dies erreicht wird. Die Empfehlungen der EDPB sollen die Datenexporteure in ihrer Beurteilung unterstützen. Nachdem der Exporteur in einem ersten Schritt geprüft hat, wohin die personenbezogenen Daten übermittelt werden und in einem zweiten Schritt überprüft hat worauf sich der Datentransfer stützt, so muss er in einem dritten Schritt beurteilen, ob in den geltenden Rechtsvorschriften und Gepflogenheiten des Drittlandes etwas vorhanden ist, dass die Wirksamkeit der angemessenen Garantien der Übermittlungsinstrumente, auf die Sie sich berufen, in Zusammenhang mit Ihrer spezifischen Übermittlung beeinträchtigen können.[272] Die Datentransfer-Folgenabschätzung muss Elemente beinhalten, die den Zugang zu Daten durch die Behörden des Drittlandes des Importeurs betreffen. Dies kann beispielsweise sein;

- wenn Behörden des Drittlandes mit oder ohne Kenntnis des Importeurs versuchen können auf die personenbezogenen Daten zuzugreifen, im Zusammenhang mit den Gesetzen, Praktiken und Präzedenzfällen.

- wenn Behörden des Drittlandes des Datenimporteurs die Möglichkeit haben, über den Datenimporteur, Telekommunikationsanbieter oder Kommunikationskanäle auf Daten zuzugreifen, basierend auf den Gesetzen, rechtlichen Befugnissen, den ihnen zu Verfügung stehenden technischen, finanziellen und personellen Ressourcen und den Präzedenzfällen.[273]

Mit in die Folgenabschätzung muss zudem einfliessen, ob die Verpflichtungen oder Befugnisse, die sich aus solchen Rechtsvorschriften und Gepflogenheiten ergeben mit den Übermittlungsinstrumenten nach Art. 46 DSGVO unvereinbar sind. Dies ist der Fall, wenn die Gesetze und Methoden des Drittlandes gegen die Grundrechte und -freiheiten der EU-Grundrechtecharta verstossen oder darüber hinausgehen, was in einer Demokratie «notwendig und verhältnismässig» ist.[274] Bei der Datentransfer-Folgenabschätzung sind jedoch nicht nur die potenziellen Risiken aufgrund bestehender Rechtsvorschriften zu beachten, sondern auch das tatsächliche Risiko für den Datentransfer.[275] Denn gemäss

[271] Vgl. Kapitel 4.1.1.
[272] EDPB, Empfehlungen 01/2020, S. 3 ff.
[273] EDPB, Empfehlungen 01/2020, Rz. 31.
[274] EDPB, Empfehlungen 01/2020, Rz. 38.
[275] SCHMITZ/SPIES, S. 1.

Klausel 14 lit. b neuer SCC-Beschluss erklären die Parteien, dass sie im Anbetracht der Zusicherung der Annahme, dass der Datenimporteur den Behörden im Drittland keine Einsichtnahme in die Daten gestattet, insbesondere technischen Details aus Ziff. i, wie beispielsweise die Übermittlungsumstände berücksichtigen. Nach Ziff. ii bestimmen die Parteien, dass sie ausdrücklich, «die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschliesslich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien» beachtet haben. Datenexporteure sollten kontrollieren, ob die Verpflichtungen die dem Datenimporteur durch das Drittland im Sinne von Gesetzesvorschriften und Praktiken auferlegt werden, die Ausübung der Rechte der betroffenen Personen nach Art. 46 DSGVO verhindern.[276] Zudem muss er überprüfen, ob die Rechtsvorschriften aufgrund welchen die Behörden des Drittlands Zugang auf personenbezogene Daten erhalten, öffentlich zugänglich und ausreichend klar definiert sind.[277]

Die Datentransfer-Folgenabschätzung muss deshalb auf öffentlich zugänglichen Rechtsbestimmungen basieren. Die Prüfung der Vorgehensweisen der Drittlandbehörden ist von besonderer Bedeutung, wenn das Drittland grundsätzlich Rechtsvorschriften hat, die den EU-Standard für die Grundrechte sowie das Verhältnismässigkeitsprinzip für deren Einschränkung gewährleistet, die Behörden diese jedoch normalerweise nicht einhalten. Oder wenn es im Drittland an Gesetzen fehlt, die einen angemessenen Schutz von personenbezogenen Daten gewährleisten. Ergibt die Prüfung, dass die Rechtsvorschriften des Drittlands problematisch sind und die übermittelten Daten in den Anwendungsbereich ebendieser heiklen Vorschriften fallen oder fallen könnten, so ist entweder die Übermittlung einzustellen, es sind zusätzliche Massnahmen zu ergreifen, um ein gleichwertiges Schutzniveau sicherzustellen oder der Transfer kann fortgeführt werden, wenn der Datenexporteur der Ansicht ist, es gebe keinen Grund zur Annahme, dass die problematischen Vorschriften auf die von ihm übermittelten Daten angewendet werden. Die Parteien müssen in einem detaillierten Bericht dokumentieren, dass die problematischen Rechtsvorschriften nicht angewendet werden und der Datenimporteur nicht an der Erfüllung seiner Verpflichtung aus Art. 46 DSGVO gehindert wird.[278]

[276] EDPB, Empfehlungen 01/2020, Rz. 39.
[277] EDPB, Empfehlungen 01/2020, Rz. 41.
[278] EDPB, Empfehlungen 01/2020, Rz. 43 ff.

5.2 Checkliste Datentransfer-Folgenabschätzung

Checkliste Datentransfer-Folgenabschätzung nach Klausel 14 des Durchführungsbeschlusses 2021/914

Gewährleistung, dass die Verpflichtungen, die dem Datenimporteur durch die USA im Sinne von Gesetzesvorschriften und Praktiken auferlegt wurden, den Datenimporteur nicht an der Erfüllung seiner Pflichten gemäss dem SCC hindern.

Diese Checkliste bezieht sich auf den Datentransfer in die USA, welche als ein Drittland ohne Angemessenheitsbeschluss nach Art. 45 DSGVO gilt.

Schritt 1: Beschreibung der Übermittlung

Folgende Aspekte der Übermittlung wurden angemessen überprüft:

	Ja	Nein	Beschreibung
Länge der Verarbeitungskette	☐	☐	
Anzahl der beteiligten Akteure	☐	☐	
Verwendete Übertragungskanäle	☐	☐	
Beabsichtigte Datenweiterleitungen	☐	☐	
Art des Empfängers	☐	☐	
Zweck der Verarbeitung	☐	☐	
Kategorie der übermittelten personenbezogenen Daten	☐	☐	
Format der übermittelten personenbezogenen Daten	☐	☐	
Wirtschaftlicher Sektor	☐	☐	
Speicherort der übermittelten Daten	☐	☐	

Schritt 2: Bewertungsgrundlage basierend auf:

- eigene, bisherige Erfahrungen mit diesem Datenimporteur
- andere zuverlässige Quellen (z.B. Rechtsgutachten, Berichte, öffentlich empfängliche Informationen)

	Ja	Nein	Beschreibung
Problematische Gesetze der USA (*insbesondere bezüglich solcher,*	☐	☐	

die die Offenlegung von Daten ggü. Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten)			
Problematische Praktiken der USA (*insbesondere bezüglich solcher, die die Offenlegung von Daten ggü. Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten)*	☐	☐	
Schritt 3: Existierende Sicherheitsmassnahmen			
	Ja	Nein	Beschreibung
Bestehen zusätzliche vertragliche Massnahmen?	☐	☐	
Bestehen zusätzliche technische Massnahmen?	☐	☐	
Bestehen zusätzliche organisatorische Massnahmen?	☐	☐	
Schritt 4: Risikobewertung			
	Ja	Nein	Beschreibung
Handelt es sich beim Datenimporteur um einen Anbieter eines elektronischen Kommunikationsdienstes bzw. unterliegt er dem US-Cloud Act?	☐	☐	
Dokumentationspflicht			
Bewahren Sie diese Checkliste auf und stellen Sie sie auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung.			

6 Schlussfolgerung

Eine der aktuell grössten Herausforderungen im Datenschutzrecht, ist die Verwendung von Cloud-Dienstleistungen aus Drittländern, welche kein angemessenes Schutzniveau bieten können. Im Laufe der vergangenen Jahre, hat sich die Tendenz der europäischen und Schweizer Datenschutzpolitik stark verändert. An die Stelle bei der früher Safe-Harbor als Angemessenheitsbeschluss den Datentransfer in die USA abgesichert hat, trat das

Privacy Shield. Es sollte die Sicherheit im Datenaustausch verbessern und somit als neue Grundlage fungieren. Jedoch wurde auch dieser Angemessenheitsbeschluss vom EuGH in ihrem bekannten Schrems II als ungültig qualifiziert. Dieses Urteil schlug in der Datenschutzwelt grosse Wellen, sorgte für hitzige Diskussionen und verunsicherte diverse Stellen bezüglich des weiteren Vorgehens mit Datentransfers von personenbezogenen Daten in die USA.

Die vorliegende Arbeit soll in kompakter Form aufzeigen, welche Optionen Unternehmen zur Verfügung stehen, die personenbezogene Daten in Clouds von US-Anbietern übermitteln, um die betroffenen Personen angemessen zu schützen und weiterhin als attraktives Unternehmen in einer digitalisierten und globalisierten Welt auf dem Markt mitwirken zu können. Aufgrund der laufenden Entwicklungen insbesondere mit dem Schrems II Urteil und der Entwicklung mit der Google Analytics Problematik zeigt sich, dass personenbezogene Daten nicht mehr ohne Aufwand in die USA transferiert werden können.

Eine Möglichkeit, um sicherzustellen, dass die US-Behörden nicht auf die personenbezogenen Daten in Clouds zugreifen können, wäre auf die Nutzung von US-Clouds gänzlich zu verzichten. Denn wo keine Daten abgespeichert sind, kann auch auf keine Daten zugegriffen werden. Dies ist wohl eine eher unrealistische Option, da die wenigstens Unternehmen in der heutigen Zeit auf eine Cloud verzichten können oder wollen und gleichwohl die Bedürfnisse aller Anspruchsgruppen befriedigen können. Freilich bieten auch europäische Unternehmen Cloud-Dienstleistungen an, jedoch werden diese selten genutzt. Die grossen Namen der Cloud Anbieter wie Microsoft, Google oder Amazon setzen sich auch auf dem hiesigen Markt durch. Bis andere technische Möglichkeiten vorhanden sind, wird der Verzicht auf US-Cloud-Dienstleister wohl kaum die richtige Lösung für eine Grosszahl von Unternehmen sein.

Als weitere Möglichkeit steht der Auftragsverarbeitervertrag mittels neuen Standardvertragsklauseln zur Verfügung. Mit diesem Instrument können die Parteien die Schutzvorschriften nach europäischem oder Schweizer Recht gewährleisten und ein angemessenes Niveau der Datensicherheit garantieren. Jedoch muss hier in Bezug auf die US-Cloud-Dienstleister der Fokus auf die technischen Massnahmen gelegt werden, da es heute noch keine ausreichenden technischen Möglichkeiten gibt, um die Daten so zu verschlüsseln, dass keine Sicherheitsbedenken bestehen und die Daten gleichzeitig durch den Exporteur ohne Probleme verarbeitet werden können.

In der Praxis ist noch eine weitere Option verfügbar, namentlich die interne Datentransfer-Folgenabschätzung. Die Gewährleistung der Parteien, dass sie keinen Grund zur Annahme haben, dass die Verarbeitung von personenbezogenen Daten durch den Cloud-Anbieter unvereinbar mit den Rechtsvorschriften und Gepflogenheiten der USA sei, ist keine einfache Angelegenheit. Diese Risikoanalyse ist mit erheblichem Aufwand verbunden und ist von Fall zu Fall unterschiedlich. Das macht eine Handhabung nicht leicht und die Tatsache, dass es keine offiziellen Richtlinien gibt, erhöht die Unsicherheit weiter. Dass diese Datentransfer-Folgenabschätzung in jedem Fall neu bestimmt werden muss, kann jedoch auch als Vorteil angesehen werden, wie auch der Umstand, dass keine offiziellen Richtlinien vorhanden sind. Dadurch können die Unternehmen selbst abschätzen, wie sicher eine US-Dienstleister für sie sein muss, damit sie seine Dienste trotzdem verwenden.

Leider besteht derzeit keine perfekte Lösung für den Transfer von personenbezogenen Daten in US-Clouds. Keine US-Clouds mehr zu nutzen ist wohl die einfachste jedoch auch die unrealistischste Option in der Praxis. Die Unternehmen, welche US-Clouds nutzen sollen in erster Linie die neuen SCC abschliessen. Darin sollten sie den technischen Massnahmen besonderes Gewicht zukommen lassen und die Datentransfer-Folgenabschätzung anhand einer Checkliste, wie sie dieser Arbeit vorliegt, punktuell abhandeln.

Bei all der Aufregung um die US-Clouds sollte nicht vergessen werden, dass diese neuen Vorschriften und Praktiken allesamt das Ziel verfolgen die betroffene Person und deren personenbezogenen Daten zu schützen, insbesondere vor Zugriffen der US-Behörden.