Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller

Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte

Utilisation des services de cloud par les avocates et avocats

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Schriften aus dem ITSL, herausgegeben von Florent Thouvenin und Rolf H. Weber

Volume 4

Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller

Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte

Utilisation des services de cloud par les avocates et avocats

Schulthess § 2019

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7255-7975-4

www.schulthess.com

Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller

Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte

Vorwort

Im Zuge der Digitalisierung nutzen Anwaltskanzleien vermehrt die Dienste von Cloud-Providern für das Bearbeiten, Speichern und Archivieren von Dokumenten und anderen Dateien. Inzwischen finden sich am Markt sogar Cloud-Dienste, die spezifisch auf die Bedürfnisse der Anwaltschaft zugeschnitten sind. Die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte wirft allerdings straf- und datenschutzrechtliche Fragen auf, die in der Lehre teilweise kontrovers beurteilt werden.

Vor diesem Hintergrund hat der Schweizerische Anwaltsverband (SAV) das Center for Information Technology, Society, and Law (ITSL) der Universität Zürich im Sommer 2018 damit beauftragt, die rechtlichen Rahmenbedingungen der Nutzung von Cloud-Diensten aus Sicht des Straf- und Datenschutzrechts näher zu untersuchen. Das ITSL hat das Gutachten im Herbst 2018 erstattet. Dem Wunsch des SAV, die Erkenntnisse des Gutachtens einer breiten Öffentlichkeit zukommen zu lassen, wird mit der Publikation einer ergänzten und aktualisierten Version in der Schriftenreihe des ITSL nachgekommen.

Die Autoren möchten sich an dieser Stelle beim SAV für die angenehme Zusammenarbeit bedanken. Für die Recherche und für Vorarbeiten an Textteilen des Gutachtens geht der Dank an MLaw Damian George, RA, MLaw, Rebecca Sigg, RAin, MSc. Bruno Rodrigues, MSc. Sina Rafati sowie MSc. Eder Scheid. Ferner sei stud. iur. Peter-Conradin Schreiber und Dr. Aurelia Tamò-Larrieux für die Durchsicht des Manuskripts und Frau Geneviève Kaspers-Grandchamp für die Übersetzung ins Französische gedankt.

Zürich, im Februar 2019

CHRISTIAN SCHWARZENEGGER
FLORENT THOUVENIN
BURKHARD STILLER

Inhaltsverzeichnis

Abkürzungsverzeichnis / Abréviations

a.F.	alte Fassung
a.M.	anderer Meinung
Abs.	Absatz
AES	Advanced Encryption Standard
AJIL	The American Journal of International Law
AJP	Allgemeine Juristische Praxis
al.	alinéa
AP-LPD	Avant-projet LPD du 21 décembre 2016
Art.	Artikel / article
ATF	Recuiel officiel des arrêts du Tribunal fédéral suisse
Aufl.	Auflage
AwR	Anwaltsrevue – Das Praxismagazin des Schweizerischen Anwaltsverbands = Revue de l'avocat
BankG	Bundesgesetz über die Banken und Sparkassen (SR. 952.0)
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BezGer	Bezirksgericht

BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGer	Bundesgericht
BGFA	Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (SR. 935.61)
BSK	Basler Kommentar
bspw.	beispielsweise
Bst.	Buchstabe
BT	Besonderer Teil
CC	Code civil suisse (RS. 210)
CCZ	Corporate Compliance Zeitschrift
ch.	chiffre
cit.	cité
CJUE	Cour de justice (Union européenne)
CL	Convention de Lugano, convention concernant la compétence judicaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (RS. 0.275.12)
Cloud Act	Clarifying Lawful Overseas Use of Data Act, 115th Congress, 2D Session, S. 2383
CO	Loi fédérale complétant le code civil suisse (RS. 220)

comp.	comparer
consid.	considération
CP	Code pénal suisse (RS. 311.0)
CPP	Code de procédure pénale suisse (RS. 312.0)
CR	Computer und Recht - Zeitschrift für die Praxis des Rechts der Informationstechnologie
d.h.	das heisst
digma	digma - Zeitschrift für Datenrecht und Informationssicherheit
Diss.	Dissertation
DSG	Bundesgesetz über den Datenschutz (SR. 235.1)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
D-StGB	Strafgesetzbuch der Bundesrepublik Deutschland
E.	Erwägungsgrund
éd.	édition

EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
E-DSG	Entwurf Bundesgesetz über den Datenschutz, BBl. 2017 7193
EEE	Espace économique européen
ég.	également
EIMP	Loi fédérale sur l'entraide internationale en matière pénale (RS. 351.1)
ErwG	Erwägungsgrund
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuZ	Zeitschrift für Europarecht
EWR	Europäischer Wirtschaftsraum
f.	und folgende
FF	Feuille fédérale
ff.	und folgende
Fn.	Fussnote
FS	Festschrift
GesKR	Zeitschrift für Gesellschafts- und Kapitalmarktrecht
h.L.	herrschende Lehre
Harv. L. Rev	Harvard Law Review

Hrsg.	Herausgeber
HTTPS	Hypertext Transfer Protocol Secure
i.V.m.	in Verbindung mit
IaaS	Infrastructure-as-a-Service
IDG	Gesetz über die Information und den Datenschutz, Kanton Zürich (LS. 170.4)
insb.	insbesondere
IP	Internet-Protokoll
IPRG	Bundesgesetz über das Internationale Privatrecht (SR. 291)
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (SR. 351.1)
IT	Informationstechnologie
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce Law
LB	Loi fédérale sur les banques et les caisses d'épargne (RS. 952.0)
LDIP	Loi fédérale sur le droit international privé (RS. 291)
let.	lettre
lit.	litera
LLCA	Loi fédérale sur la libre circulation des avocats (RS. 935.61)

LPD	Loi fédérale sur la protection des données (RS. 235.1)
LugÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, Lugano-Übereinkommen (SR. 0.275.12)
m.N.	mit Nachweisen
m.w.H.	mit weiteren Hinweisen
medialex	Zeitschrift für Kommunikationsrecht
MMR	MultiMedia und Recht
N	note
No.	number
OGer	Obergericht
OLPD	Ordonnance relative à la loi fédérale sur la protection des données (RS. 235. 11)
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht, SR. 220)
Ö-StGB	Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB)
p. ex.	par exemple

PaaS	Platform-as-a-Service
PFPDT	Préposé fédérale à la protection des données et à la transparence
PJA	Pratique Juridique Actuelle
PK	Praxiskommentar
P-LPD	Projet-LPD
RDS	Revue de droit suisse
réf.	références
RGDP	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) = DSGVO
Rn.	Randnummer
Rz.	Randziffer
s.	suivant
SaaS	Software-as-a-Service
SHK	Stämpflis Handkommentar
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SJ	La Semaine Judicaire

SJZ	Schweizerische Juristen Zeitung
SSL	Secure Socket Layer
Stan. L. Rev. Online	Stanford Law Review Online
StGB	Schweizerisches Strafgesetzbuch (SR. 311.0)
StPO	Schweizerische Strafprozessordnung (SR. 312.0)
SZS	Schweizerische Zeitschrift für Sozialversicherung und berufliche Vorsorge
TF	Tribunal fédéral
TLS	Transport Layer Security
UE	Union européenne
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR. 235.11)
VE-DSG	Vorentwurf eines totalrevidieren Schweizer Datenschutzgesetzes vom 21. Dezember 2016
vgl.	vergleiche
Vol.	Volume
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutzrecht
ZGB	Schweizerisches Zivilgesetzbuch (SR. 210)
zit.	zitiert

ZR	Blätter für Zürcherische Rechtsprechung
ZSR	Zeitschrift für Schweizerisches Recht
ZStrR	Zeitschrift für Strafrecht

Literaturverzeichnis / Bibliographie

ALTHAUS STÄMPFLI ANNETTE, Kundendaten von Banken und Finanzdienstleistern, Datenschutz und Bankgeheimnis versus Offenlegungspflicht und Outsourcing, 2. Aufl., Bern 2009

AZZI ADÈLE, The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law 2018, Vol. 9(2), 126–137

BAERISWYL BRUNO/PÄRLI KURT (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, Bern 2015 (zit: SHK-DSG, BEARBEITER)

BAERISWYL BRUNO/RUDIN BEAT (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012 (zit: BEARBEITER, in: Baeriswyl/Rudin)

BENHAMOU YANIV/JACOT-GUILLARMOD EMILIE, RGPD sur sol suisse: mise en oeuvre, digma 2018, 142–149

BERGER BERNHARD, Outsourcing vs. Geheimnisschutz im Bankgeschäft, recht 2000, 182–197

BLASS HEINZ W., Ältere und neuere Probleme der Pflicht zur Wahrung des «Berufsgeheimnisses», SJZ 1966, 337–343

BOHNET FRANCOIS/MARTENET VINCENT, Droit de la profession d'avocat, Bern 2009

BÜHLMANN LUKAS/REINLE MICHAEL, Extraterritoriale Wirkung der DSGVO, digma 2017, 8–12

CHAPPUIS BENOÎT, La profession d'avocat, Le cadre légal et les principes essentiels, Tome I, 2. Aufl., Zürich 2016

CHAPPUIS BENOÎT/ALBERINI ADRIEN, Secret professionnel de l'avocat et solutions Cloud, AwR 2017, 337–343

CORBOZ BERNARD, Le secret professionnel de l'avocat selon l'art. 321 CP, SJ 1993, 77–108

CORBOZ BERNARD, Les infractions en droit suisse, Vol. II, 3. Aufl., Bern 2010

CORDING SEBASTIAN/GÖTZINGER LENA, Der CLOUD Act aus europäischer Sicht, CR 2018, 636–640

DASKAL JENNIFER, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review Online 2018, Vol. 71, 9–16

DE LA CRUZ CARMEN, Cloud Computing – Alter Wein in neuen Schläuchen?, Jusletter IT 15. Mai 2013

DE HALLER GENEVIÈVE, Le secret médical en matière d'assurance, Schweizerische Versicherungs-Zeitschrift 1980, 6–21

DONATSCH ANDREAS (Hrsg.), StGB, JStG Kommentar, Orell Füssli Kommentar, 20. Aufl., Zürich 2018 (zit: BEARBEITER, StGB/JStGB-Kommentar)

DONATSCH ANDREAS/THOMMEN MARC/WOHLERS WOLFGANG, Strafrecht IV: Delikte gegen die Allgemeinheit, in: Jositsch (Hrsg.) Zürcher Grundrisse des Strafrechts, 5. Aufl., Zürich 2017

DUPUIS MICHEL/MOREILLON LAURENT/PIGUET CHRISTOPHE/BERGER SÉVERINE/MAZOU MIRIAM/RODIGARI VIRGINIE, Petit Commentaire, CP Code pénal, 2. Aufl., Basel 2017

DYENS ALEXANDRE, Territorialité et ubiquité en droit pénal international suisse, Étude critique des art. 3 et 8 CPS? Enjeux théoriques et pratiques, en particulier en matière de criminalité économique et financière, Basel 2014

ECKHARDT JENS, DS-GVO: Anforderungen an die Auftragsdatenverarbeitung als Instrument zur Einbindung Externer, CCZ 2017, 111–117

EHMANN EUGEN/SELMAYR MARTIN (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, 2. Aufl., München 2018 (zit: BEARBEITER in: Ehmann/Selmayr)

EICKER ANDREAS, Der räumliche und zeitliche Geltungsbereich des nationalen Wirtschaftsstrafrechts, in: Ackermann/Heine (Hrsg.), Wirtschaftsstrafrecht der Schweiz: Hand- und Studienbuch, Bern 2013, 57–81

EPINEY ASTRID, Allgemeine Grundsätze, in: Belser/Epiney/Waldmann, Datenschutzrecht: Grundlagen und öffentliches Recht, Bern 2011, 510–558

FELLMANN WALTER, Anwaltsrecht, 2. Aufl., Bern 2017

FELLMANN WALTER/ZINDEL GAUDENZ G., Kommentar zum Anwaltsgesetz: Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) BGFA, 2. Aufl., Zürich/Basel/Genf 2011 (zit: BEARBEITER, in: Fellmann/Zindel)

FISCHER ANDREA, Sensible Daten in fremden Händen, Tages-Anzeiger, 11. Januar 2016, <https://www.tagesanzeiger.ch/wirtschaft/sozial-und-sicher/Sensible-Daten-in-fremden-Haenden/story/16103347>, zuletzt besucht am 30. Oktober 2018

FISCHER JOEL/BORNHAUSER JONAS, Elektronische Board Portale: Hosted in Switzerland als neuer rechtlicher Qualitätsstandard, GesKR 2016, 425–448

GALBRAITH JEAN, Contemporary Practice of the United States relating to International Law, The American Journal of International Law 2018, Vol. 112(3), 486–493

GAUSLING TINA, Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, 578–582

GEORGE DAMIAN/TAMÒ AURELIA, Ein Europäisches Recht auf Vergessen – eine Schweizer Pflicht zum Löschen?, in: Brändli/Schister/Tamò (Hrsg.), Multinationale Unternehmen und Unternehmen im Wandel – Herausforderung für Wirtschaft, Recht und Gesellschaft, Bern 2013, 31–56

GLESS SABINE, Internationales Strafrecht, 2. Aufl., Basel 2015

GOLA PETER (Hrsg.) Datenschutz-Grundverordnung: VO (EU) 2016/679), Kommentar, 2. Aufl., München 2018 (zit: BEARBEITER, in: Gola)

GRAMIGNA RALPH, Cloud-Vertrag, in: Münch/Kasper Lehne/Probst (Hrsg.), Schweizerisches Vertragshandbuch: Musterverträge für die Praxis, 3. Aufl., Basel 2017 (zit: GRAMIGNA, Cloud-Vertrag)

GRAMIGNA RALPH, Datenschutz und Outsourcing, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 759–786 (zit: GRAMIGNA, Datenschutz und Outsourcing)

HAFTER ERNST, Lehrbuch des schweizerischen Strafrechts, Allgemeiner Teil, 2. Aufl., Bern 1946

HOEREN THOMAS, Bedeutung der europäischen Datenschutzgrundverordnung für die Schweiz unter besonderer Berücksichtigung der Pflicht zur Bestellung eines Vertreters nach Art. 27 DSGVO, EuZ 2018, 162–166

HONSELL HEINRICH/VOGT NEDIM-PETER/SCHNYDER ANTON K./BERTI STEPHEN (Hrsg.), IPR Basler Kommentar, 3. Aufl., Basel 2013 (zit: BSK-IPRG, BEARBEITER)

HONSELL HEINRICH/VOGT NEDIM PETER/WIEGAND WOLFGANG (Hrsg.), Basler Kommentar OR I, 6. Aufl., Basel 2015 (zit: BSK-OR I, BEARBEITER)

HONSELL HEINRICH/VOGT NEDIM PETER/GEISER THOMAS (Hrsg.), Basler Kommentar ZGB I, 5. Aufl., Basel 2014 (zit: BSK-ZGB I, BEARBEITER)

HÖPFEL FRANK/RATZ ECKART (Hrsg.), Wiener Kommentar zum Strafgesetzbuch, 184. Lieferung, 2. Aufl., Wien 2017 (zit: Wiener Kommentar, BEARBEITER)

KELLER KARIN, Das ärztliche Berufsgeheimnis gemäss Art. 321 StGB unter besonderer Berücksichtigung der Regelung im Kanton Zürich, Diss., Zürich 1993

KÜHLING JÜRGEN/BUCHNER BENEDIKT, Datenschutzgrundverordnung/BDSG, 2. Aufl., München 2018 (zit: BEARBEITER, in: Kühling/Buchner)

LANGMACK HANS, Die strafrechtliche Schweigepflicht des Arztes, ZStrR 1972, 67–80

LAUE PHILIP/NINK JUDITH/KREMER SASCHA, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016

LAUE PHILIP, Öffnungsklauseln in der DS-GVO – Öffnung wohin?: Geltungsbereich einzelstaatlicher (Sonder)Regelungen, ZD 2016, 463–467

MACALUSO ALAIN/MOREILLON LAURENT/QUELOZ NICOLAS (eds.), Commentaire Romand, Code pénal II, Basel 2017 (zit: CR-CP II, BEARBEITER)

MAURER-LAMBROU URS/BLECHTA GABOR (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit: BSK-DSG/BGÖ, BEARBEITER)

MÉTILLE SYLVAIN, Confier ses données à une société étrangère n'est pas sans risque, medialex 2013, 63–64

MUGGLI, SANDRA, Im Netz ins Netz – Pädokriminalität im Internet und der Einsatz von verdeckten Ermittlern und verdeckten Fahndern zu deren Bekämpfung, Zürich 2014

NIGGLI MARCEL ALEXANDER, Unterstehen dem Berufsgeheimnis nach Art. 321 StGB auch Unternehmensjuristen? Eine Verteidigung des materiellen Strafrechts gegen die Freunde des Verfassungsrechts, zugleich eine Antwort auf Pfeifer, AwR 2006, 277–280

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, 3. Aufl., Basel 2013 (zit: BSK-Strafrecht I, BEARBEITER)

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht II, 3. Aufl., Basel 2013 (zit: BSK-Strafrecht II, BEARBEITER)

PASSADELIS NICOLAS, Rechtsanwendung bei internationalen Datenbearbeitungen durch Private, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, 167–201

PFEIFER MICHAEL, Gilt das Berufsgeheimnis nach Art. 321 StGB auch für Unternehmensjuristen? Der Wunsch als Vater des Gedankens oder Realistik der Auslegung? AwR 2006, 166–170

PIETH MARK, Strafrecht, Besonderer Teil, 2. Aufl., Basel 2018

PLATH KAI-UWE (Hrsg.), BDSG/DSGVO, Kommentar, 2. Aufl., Köln 2016 (zit: BEARBEITER, in: Plath)

PRAZ EMILIE M., Responsabilités et outils de conformité selon la RGPD: Obligations du responsable de traitement et du sous-traitant, AJP 2018, 609–616

PROBST THOMAS, Die unbestimmte "Bestimmbarkeit" der von Daten betroffenen Person im Datenschutzrecht, AJP 2013, 1423–1436

RASELLI NICCOLÒ, Amts- und Rechtshilfe durch Informationsaustausch zwischen schweizerischen Straf- und Steuerbehörden, ZStrR 1993, 26–55

REHBERG JÖRG, Arzt und Strafrecht, in: Honsell (Hrsg.), Handbuch des Arztrechts, Zürich 1994, 303–361

REHBERG JÖRG, Die strafrechtliche Seite des ärztlichen Berufsgeheimnisses, in: Schweizerische Ärztezeitung 1969, 231–236

REHMANN MERET, Grenzen vertraglicher Haftungsbeschränkungen, SJZ 2017, 129–138

RIEDO CHRISTOF, Der Strafantrag, Basel 2004

ROBRAHN RASMUS/BREMERT BENJAMIN, Interessenkonflikte im Datenschutzrecht: Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, 291–297

ROSENTHAL DAVID, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter 20. Februar 2017

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz: Was uns erwartet und was noch zu korrigieren ist, Jusletter 27. November 2017

ROSENTHAL DAVID, Datenschutz im IT-Outsourcing, Weber/Berger/Auf der Maur (Hrsg.), IT-Outsourcing, ICT: Rechtspraxis I, Zürich/Basel/Genf 2003, 193–226 (zit: ROSENTHAL, Datenschutz im IT-Outsourcing)

ROSENTHAL DAVID/KAISER BARBARA, Datenschutz: Wie weiter mit Datenübermittlungen in die USA?, Jusletter 2. November 2015

ROSENTHAL DAVID/JHÖRI YVONNE, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit: BEARBEITER, in: Rosenthal/Jhöri)

ROSSEL JEAN-EMMANUEL, Le secret médical et le certificat d'arrêt de travail, SZS 1992, 243–267

RUSSEK RENÉ, Das ärztliche Berufsgeheimnis, Diss., Zürich 1954

RÜPKE GISELHER/VON LEWINSKI KAI/ECKHARDT JENS, Datenschutzrecht: Grundlagen und europarechtliche Neugestaltung, München 2018

SCHÄFER PETER, Ärztliche Schweigepflicht und elektronische Verarbeitung, Diss., Zürich 1978

SCHILLER KASPAR, Schweizerisches Anwaltsrecht, Zürich/ Basel/Genf 2009

SCHMID NIKLAUS, Computer- sowie Check- und Kreditkarten-Kriminalität, Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994

SCHMIDT BERND/FREUND BERNHARD, Perspektiven der Auftragsdatenverarbeitung – Wegfall der Privilegierung mit der DS-GVO?, ZD 2017, 14–18

SCHÖNKE ADOLF/SCHRÖDER-LENCKNER HORST, StGB-Kommentar, 27. Aufl., München 2006 (zit: BEARBEITER, in Schönke/Schröder, 27. Aufl.)

SCHWANINGER DAVID/LATTMANN STEPHANIE S., Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, Jusletter 11. März 2013

SCHWARZENEGGER CHRISTIAN, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht – ein leading case zu grenzüberschreitenden Internetdelikten, sic! 2001, 240–252

SCHWARZENEGGER CHRISTIAN, Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht, ZSR 2008 II, 399–503

SCHWARZENEGGER, CHRISTIAN, Der räumliche Geltungsbereich des Strafrechts im Internet, ZStrR 2000, 109–130

SCHWARZENEGGER CHRISTIAN, E-Commerce – Die strafrechtliche Dimension, in: Arter/Jörg (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen 2001, 329–375 (zit: SCHWARZENEGGER, E-Commerce)

SEELMANN KURT/GETH CHRISTPOHER, Strafrecht Allgemeiner Teil, 6. Aufl., Basel 2016

SIDLER IRIS/VASELLA DAVID, Aus Safe Harbor wird Privacy Shield: Folgen des Urteils des EuGH i.S. Schrems, sic! 2016, 185–195

SIEBEN ALEXANDER, Das Berufsgeheimnis auf Grund des eidgenössischen Strafgesetzbuches, Diss. Bern 1943

SIMITIS SPIROS, „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion, in: Brem/Druey/Kramer/Schwander (Hrsg.), Festschrift für Mario M. Pedrazzini, Bern 1990, 469–493

SPINDLER GERALD/SCHMECHEL PHILIPP, Personal Data and Encryption in the European General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law 2016, Vol. 7(2), 163–177

STAIGER DOMINIC N., Data Protection Compliance in the Cloud, Zürich 2017

STEIGER MARTIN, Neues EU-Datenschutzrecht: Was gilt für Anwaltskanzleien?, AwR 2018, 205–211

STOCKER CHRISTOPH, Regulatorische Anforderungen an IT-Outsourcing: Finanzmarktbereich, in: Weber/Berger/Auf der Maur (Hrsg.), IT-Outsourcing, ICT: Rechtspraxis I, Zürich 2003, 227–253

STOCKER WERNER, Das Anwaltsgeheimnis, ZStrR 1953, 1–18

STRATENWERTH GÜNTER, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 4. Aufl., Bern 2011

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7. Aufl., Bern 2013

STRATENWERTH GÜNTER/WOHLERS WOLFGANG, Schweizerisches Strafgesetzbuch Handkommentar, 3. Aufl., Bern 2013

STRAUB WOLFGANG, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP 2010, 547–564

STRAUB WOLFGANG, Cloud Verträge – Regelungsbedarf und Vorgehensweise, AJP 2014, 905–923

SURY URSULA/GOGNIAT YVES, Umzug einer Kanzlei in die Cloud, AwR 2015, 201–206

SYDOW GERNOT (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit: BEARBEITER, in: Sydow)

THALMANN ANDRÉ, Zur Anwendung des schweizerischen Datenschutzgesetzes auf internationale Sachverhalte, sic! 2007, 337–343

TIMM MANFRED, Grenzen der ärztlichen Schweigepflicht, Diss., Düsseldorf 1988

TSCHÄNI RUDOLF/DIEM HANS-JAKOB, Interessenkonflikte in M&A-Transaktionen, in: Tschäni (Hrsg.), Mergers & Acquisitions XVIII, Zürich 2016, 53–144

TRECHSEL STEFAN/PIETH MARK (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 3. Aufl., Zürich 2018 (zit: PK-StGB, BEARBEITER)

UTTINGER URSULA/LIEBRENZ MICHAEL, Nutzung medizinischer Schreibservices – eine datenschutzrechtliche Sicht, Schweizerische Ärztezeitung 2014, 1745–1747

VALTICOS MICHEL/REISER CHRISTIAN M./CHAPPUIS (Hrsg.), Commentaire romand, Loi sur les avocats, LLCA, Basel 2010 (zit: CR-LLCA, BEARBEITER)

VASELLA DAVID, Zum Anwendungsbereich der DSGVO, digma 2017, 220–222

VLCEK MICHAEL, Cross Border Cloud Computing und Discovery-Risiken, in: Grosz/Grünewald (Hrsg.), Recht und Wandel, Festschrift für Rolf H. Weber, Zürich 2016, 165–180

WAGNER DOMINIK/ZWIRNER SONIA, Cyber Risk in Anwaltskanzleien – Schlussfolgerungen aus dem Panama-Papers-Skandal, in: Staub (Hrsg.), Beiträge zu aktuellen Themen an der Schnittstelle zwischen Recht und Betriebswirtschaft III, Law & Management Praxis Bd. 7, Zürich 2017, 161–184

WIDMER BARBARA, Auftragsdatenbearbeitung – zum Ersten, digma 2014, 26–34

WOHLERS WOLFGANG, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zürich 2016

WOHLERS WOLFGANG, Outsourcing durch Berufsgeheimnisträger, digma 2017, 114–117

WOHLERS WOLFGANG/LYNN VERONICA, Das Anwaltsgeheimnis bei internen Untersuchungen, recht 2018, 9–24

WOLFFERS FELIX, Der Rechtsanwalt in der Schweiz – seine Funktion und öffentlich-rechtliche Stellung, Diss. Bern, Zürich 1986

ZÜRCHER EMIL, Schweizerisches Strafgesetzbuch, Erläuterungen zum Vorentwurf vom April 1908, Bern 1914

Materialien / Documents

BUNDESAMT FÜR JUSTIZ, Kommentar des Bundesamts für Justiz zur Vollzugsverordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, RS 235.11), 1. Januar 2008 (zit: BUNDESAMT FÜR JUSTIZ, Kommentar VDSG)

BUNDESAMT FÜR STATISTIK, Cloud-Computing und private Internetnutzung, Ergebnisse der «IKT-Haushaltserhebung 2014», Neuchâtel 2015

DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Tätigkeitsbericht 2017 (zit: DSB ZÜRICH, Tätigkeitsbericht 2017)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER, EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015 (zit: EDÖB, Leitfaden Massnahmen des Datenschutzes)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER, Die Datenübermittlung ins Ausland kurz erklärt, Januar 2017 (zit: EDÖB, Datenübermittlung ins Ausland)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER, Stand des Datenschutzes weltweit, 12. Januar 2017, (zit: EDÖB, Staatenliste)

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER, 14. Tätigkeitsbericht 2006/2007 für den Zeitraum zwischen 1. April 2006 und 31. März 2007, (zit: EDÖB, 14. Tätigkeitsbericht)

NIGGLI MARCEL ALEXANDER, Gutachten betreffend Anwendung von Art. 321 StGB auf angestellte Unternehmensjuristen (In-house lawyers), Freiburg 2005, «Geheimsphäre des Berechtigten», <www.swissholdings.ch/fileadmin/kundendaten/Dokumente/Archiv_Publikationen-Publikation/05-08-05-Gutachten_Niggli.pdf>, zit: NIGGLI, Gutachten Unternehmensjuristen

Schweizerisches Strafgesetzbuch: Protokoll der zweiten Expertenkommission, Luzern 1915, Bd. 4 (teilw. zit: EXPERTE, in: Protokoll der zweiten Expertenkommission Strafgesetzbuch)

I. Ausgangslage und Fragestellung

Die Nutzung von IT-Diensten ist aus der Anwaltspraxis längst nicht mehr wegzudenken. Neben dem Einsatz von Software zur Textverarbeitung gehören auch die Nutzung von Softwarelösungen für das Mandatsmanagement, die Leistungserfassung und die Rechnungstellung sowie der Gebrauch von Online-Datenbanken zur Grundausstattung von Anwältinnen und Anwälten.

Am weitesten verbreitet sind bisher lokale Lösungen, entweder in Form von «*stand alone*»-Computern oder mittels lokaler Netzwerke. Die im Rahmen der beruflichen Tätigkeit von Klienten erhaltenen und die von den Anwältinnen und Anwälten produzierten Daten – etwa Verträge, Rechtsschriften und Korrespondenz – werden dabei entweder auf der Festplatte des «*stand alone*»-Rechners oder auf einem zentralen Server der Anwaltskanzlei bearbeitet und gespeichert. Das Aufsetzen und die Wartung der erforderlichen Hardware und das Installieren und Aktualisieren der Software werden in aller Regel nicht von den Anwältinnen und Anwälten selbst vorgenommen, sondern einem internen IT-Mitarbeiter oder einem externen IT-Dienstleister übertragen. Die internen IT-Mitarbeiter und diejenigen des IT-Dienstleisters erhalten im Rahmen ihrer Tätigkeit unvermeidlich Zugang zu Daten, die dem anwaltlichen Berufsgeheimnis unterstehen.

In jüngerer Zeit sind Anwaltskanzleien zunehmend dazu übergegangen, anstelle von lokalen Lösungen die Dienste von Cloud-Providern zu nutzen.

Vor diesem Hintergrund ist im Auftrag des schweizerischen Anwaltsverbands (SAV) mit dem vorliegenden Gutachten zu untersuchen, ob und gegebenenfalls unter welchen Voraussetzungen in der Schweiz tätige Anwältinnen und Anwälte im Rahmen der Ausübung ihrer beruflichen Tätigkeit für das Bearbeiten, Speichern und Archivieren von Dokumenten und anderen Dateien Cloud-Dienste nutzen,

also Dritte beiziehen dürfen, die ihnen über das Internet zugängliche Speicher- und Rechenkapazitäten zur Verfügung stellen.

Im Vordergrund stehen dabei zwei Fragestellungen: Zum einen ist zu prüfen, ob die Nutzung von Cloud-Diensten eine Verletzung des Berufsgeheimnisses der Anwältinnen und Anwälte darstellt (III). Zum anderen ist zu prüfen, ob und unter welchen Voraussetzungen die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte mit den Vorgaben des Datenschutzrechts vereinbar ist (IV). Vorab sind jedoch die technischen Grundlagen zu klären (II).

II. Technische Grundlagen

1. Cloud-Computing im Allgemeinen

Der Begriff «Cloud» beschreibt eine Reihe von Online-Diensten, die über ein Netzwerk von fast allen Standorten aus zugänglich sind, so dass der Dienstnehmer den physischen Standort dieser Dienste nicht kennt. Einer dieser Dienste kann das «Abspeichern» sein, so dass sich eine Cloud (im Gegensatz zu einem «*stand alone*»-Rechner) als dezentrales und verteiltes Speichersystem betrachten lässt, in dem alle Daten in elektronischer Form – und ohne dediziertes Format – gespeichert werden können. Zudem wird das Teilen von Daten erleichtert, da technologieunabhängige Lösungen (insb. unabhängig von Hardware und Software-/Betriebssystemen) zur Verfügung stehen. Die sog. Cloud-basierte Virtualisierung kann Unternehmen dabei helfen, die Anzahl der Maschinen (die typischerweise als getrennte Computer oder Systeme gezählt werden) und Softwarelizenzen, die sie für den Betrieb benötigen, zu reduzieren. Clouds führen damit regelmässig zu einer effizienteren und kostengünstigeren Art der Ausführung oder Unterstützung von wiederkehrenden Aufgaben und Geschäftsabläufen.

Nahezu alle IT-(Informationstechnologie)-Ressourcen (Daten sowie Hard- und Software) können in eine Cloud ausgelagert werden: ein Programm, eine Anwendung, ein Dienst, ein zweckbestimmtes Betriebssystem oder eine gesamte Infrastruktur. Möchte eine Anwaltskanzlei bspw. eine IT-Infrastruktur für den Umgang mit Dokumenten und Daten ihrer Klienten einrichten, können Software, Dienste und eine Netzwerkressource in einer Cloud eingerichtet werden. Die Anwaltskanzlei und bei Bedarf auch autorisierte Dritte (sofern geeignete Zugangskontrollen eingerichtet werden) können so über die Cloud-Infrastruktur auf die Dokumente und Daten zugreifen.

In Abbildung 1 betreiben die Anwaltskanzleien 1 und 2 die lokale Infrastruktur für ihre Mitarbeiter. Die vorliegend durchgeführte

«Cloudification» ermöglicht die Speicherung der Daten bei einem sog. Cloud-Provider, eine spezifische Instanz des IT-Dienstleisters, welcher sich auf einen zuverlässigen, vertrauenswürdigen und typischerweise effizienten Schreib- und Lesezugriff auf den Datenspeicher spezialisiert hat. Die typischerweise in Dokumenten organisierten Daten werden auf der Seite der Anwaltskanzlei verschlüsselt (gekennzeichnet durch das Schloss neben dem Dokumentensymbol), wobei die Schlüssel nur der Anwaltskanzlei oder gar einem einzelnen Nutzer dort bekannt sind. Die Daten werden dann über das Netzwerk – hier das öffentliche Internet – verschlüsselt übertragen. In diesem Beispiel wird deutlich, dass die beiden Anwaltskanzleien mit ihren eigenen Schlüsseln arbeiten, die nur der jeweiligen Kanzlei bekannt sind, aber dennoch beide Kanzleien den gleichen Cloud-Provider verwenden. Die Daten werden in der Infrastruktur des Cloud-Providers also verschlüsselt gespeichert, so dass der Cloud-Provider – oder ein Dritter – keine realistische Chance hat, den Inhalt dieser Daten zu entschlüsseln.

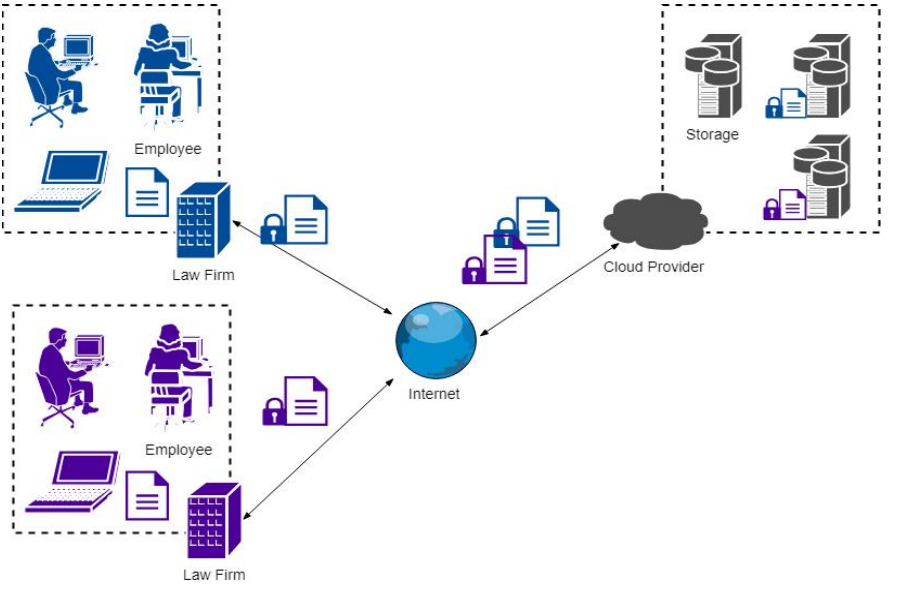

Abbildung 1: Grundsätzliche Funktionsweise des Cloud-Computing

Auch wenn die Daten der Anwaltskanzleien 1 und 2 in der gleichen Cloud-Provider-Infrastruktur gespeichert sind, kann keine Kanzlei auf die Daten der jeweils anderen Kanzlei zugreifen, weil sie nicht weiss, an welcher Stelle in der Cloud beim Cloud-Provider die Daten liegen und auch nicht über den Schlüssel zum Entschlüsseln der Daten verfügt. Sollte die Cloud-Provider-Infrastruktur kompromittiert werden, haben die offengelegten Daten ohne den richtigen Schlüssel keine Aussagekraft. Wie bei allen in der digitalen Welt verwendeten Verschlüsselungsmethoden und Berechtigungsnachweisen besteht die theoretische Wahrscheinlichkeit, dass der Schlüssel durch Dritte ermittelt werden kann; sie tendiert beim Einsatz starker Sicherheitsmechanismen jedoch gegen Null. Das Sicherheitsrisiko ist vergleichbar mit jenem von analogen Tresoren und Schliessfächern, die mit einer Zahlenkombination geöffnet werden können, die erraten oder gestohlen werden kann.

2. Cloud-Dienstmodelle

Das Cloud-Dienstmodell bestimmt, wie der konfigurierbare Satz von Cloud-Computing-Ressourcen organisiert und dem Benutzer zur Verfügung gestellt wird. Das National Institute of Standards and Technology (NIST), die Cloud Security Alliance (CSA) und die European Union Agency for Network and Information Security (ENISA) haben diese Dienste in drei Hauptkategorien unterteilt: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS). Siehe dazu Abbildung 2:

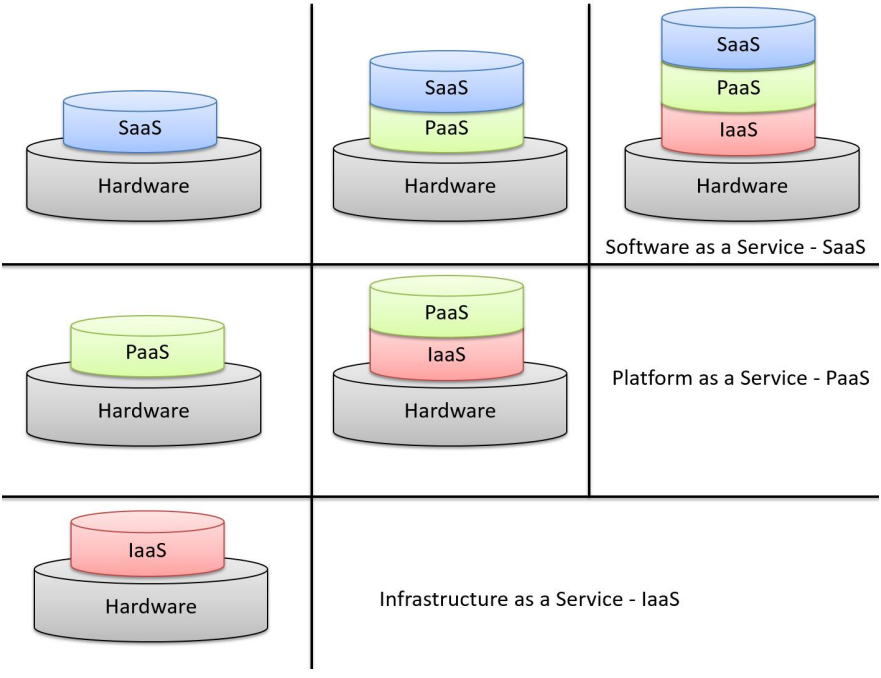

Abbildung 2: Cloud-Computing Dienstmodelle

Grundlage jeder Cloud-Dienstleistung sind die Server. Sie stellen die Hardware dar, auf der alle Dienstvariationen implementiert sind. Das IaaS-Modell, das die grundlegendste Variante der Cloud-Dienste darstellt, wird durch virtuelle Maschinen («*Virtual Machines*») bereitge-

stellt, bei denen der Benutzer nicht nur die zu verwendende Konfiguration, sondern auch die Art des Dienstes (z.B. Rechnen, Speichern oder Netzwerkzugang) wählen kann. Eine virtuelle Maschine ist eine Softwareabstraktion eines physischen Servers, welche die notwendige Umgebung für den Betrieb von Benutzeranwendungen bereitstellt. Im IaaS-Modell kann ein Benutzer eine oder mehrere virtuelle Maschinen anfordern, die auf einem oder mehreren Servern der Cloud-Provider-Infrastruktur gehostet werden (vgl. Hardware in Abbildung 2).

Das PaaS-Modell kann in zwei Arten angeboten werden: (1) Als Plattform, welche das Support- und Management-Framework für Cloud-Anwendungen enthält, also typischerweise Tools zur Entwicklung, Wartung und Aktualisierung von Anwendungen, oder (2) als Plattform in Kombination mit einer Infrastruktur (IaaS), auf der die entwickelten Anwendungen gehostet werden.

SaaS-Dienste können auf drei verschiedene Arten angeboten werden: (1) ausschliesslich als Hosting einer Anwendung, (2) als Hosting einer Anwendung in Kombination mit PaaS oder (3) als Kombination von PaaS und IaaS.

Die drei verschiedenen Dienstmodelle charakterisieren das Angebot in jeder Abstraktionsschicht des Cloud-Dienstes und machen spezifischere Modelle für eine oder mehrere dieser drei Dienstkategorien möglich. Darüber hinaus können diese Dienstmodelle sowie die hierzu erforderlichen Ressourcen (wie ebenfalls in Abbildung 2 dargestellt) auf verschiedene Weise gebündelt werden. Entsprechend ist es möglich, einen Cloud-Dienst auf der Basis eines anderen Cloud-Dienstes oder einer bestimmten Infrastruktur zur Verfügung zu stellen.

2.1 Software-as-a-Service (SaaS)

Das Software-as-a-Service (SaaS)-Dienstmodell stellt einen Cloud-Computing-Dienst zur Verfügung, d.h. eine endverbraucherfreundli-

che, Web-basierte Anwendung. In diesem Modell verwaltet oder kontrolliert eine Anwaltskanzlei nicht die zugrundeliegenden Dienste, sondern lediglich die Anwendung selbst (bspw. in Form einer Textverarbeitung, von Präsentationsfolien oder eines Fakturierungsprogramms). Alle dazugehörige Software und Daten werden auf der Cloud-Infrastruktur zentral gespeichert, was das Cloud-Management und den Support für Anwendungen erleichtert.

2.2 Platform-as-a-Service (PaaS)

Beim PaaS-Dienstmodell stellt der Cloud-Provider den Nutzern Hardware und Entwicklungstools für das Erstellen, Testen und Bereitstellen von Applikationen zur Verfügung. Der Zweck dieses Modells ist es, die Kosten und die Komplexität der darunterliegenden Hardware zu reduzieren. Die auf einer PaaS entwickelten Anwendungen sind in der Regel ausschliesslich auf den PaaS-Anbieter abgestimmt, so dass diese Anwendungen nur über die Plattform des Cloud-Providers angeboten werden können, wodurch ein «*lock-in*»-Effekt entsteht.

Das PaaS-Dienstmodell wird zur Entwicklung von Applikationen eingesetzt, weshalb derzeit nicht davon auszugehen ist, dass Anwaltskanzleien dieses Modell nutzen. Möglich ist allerdings, dass der Softwareanbieter einer Kanzlei auf ein PaaS-Dienstmodell zurückgreift.

2.3 Infrastructure-as-a-Service (IaaS)

Beim IaaS-Dienstmodell werden die Cloud-Computing-Ressourcen (z.B. Rechnen, Speichern oder Netzwerkzugang) als Dienstleistung zur Verfügung gestellt. IaaS ist das Grundmodell der Cloud-Dienstleistungen. Dieses Modell ist eine interessante Option für Unternehmen, die eine rechnergestützte Infrastruktur, bspw. ein Rechenzentrum, benötigen, diese Infrastruktur aber aus Kostengründen nicht selber betreiben können. Die hohen Unterhaltskosten für Rechenzentren und die Nachfrage nach kostengünstigeren Lösungen

haben dazu geführt, dass ein breites Angebot von spezialisierten IaaS-Anbietern besteht, die je nach Bedarf Wartungs- und Managementaufgaben (Bereitstellung eines physischen Standortes, Klimatisierung, Konnektivität, Elektrizität, Netzwerk, physische und logische Sicherheit) übernehmen und es dem Nutzer ermöglichen, sich auf sein Tagesgeschäft zu konzentrieren.

IaaS ist für eine Anwaltskanzlei interessant, wenn sie Software verwenden möchte, die nicht über ein SaaS-Dienstmodell angeboten wird und wenn sie die rechnergestützte Infrastruktur nicht selbst betreiben will. So kann eine Anwaltskanzlei bspw. jede Software einschliesslich Betriebssystem nutzen, ohne die Basisinfrastruktur der Cloud kontrollieren oder verwalten zu müssen.

3. Sicherheitsmassnahmen im Cloud-Modell

Anwaltskanzleien, die an einer Cloud-Lösung interessiert sind, haben die Wahl zwischen unterschiedlichen Cloud-Modellen. Einerseits kann eine Kanzlei lediglich eine Infrastruktur (IaaS) mieten und deren dedizierte Speicher einsetzen oder eine komplette Cloud-Speicherlösung hinzumieten, ohne sich um technische Details kümmern zu müssen (Szenario 1). Dieses Modell bietet sich an, wenn allein das Speichern von Dateien gewünscht ist. Anwaltskanzleien können aber auch an einer cloud-basierten Verarbeitung von Dateien interessiert sein. In diesem Fall kann die Kanzlei cloud-basierte Computing-Lösungen (SaaS) erwerben, um bspw. Textverarbeitung, Tabellenkalkulation, das Erstellen von Präsentationsfolien oder die Fakturierung auf in der Cloud gespeicherten Dateien auszuführen (Szenario 2). Dabei kann eine massgeschneiderte oder eine dedizierte («*commercial off-the-shelf*») Anwendung gewählt werden.

3.1 SaaS-, PaaS- und IaaS-Sicherheitsmassnahmen

Die Wahl des Dienstmodells hat auf die notwendigen Sicherheitsmassnahmen («*Security Measures*») einen grossen Einfluss. Abbildung 3 stellt diesen Zusammenhang dar.

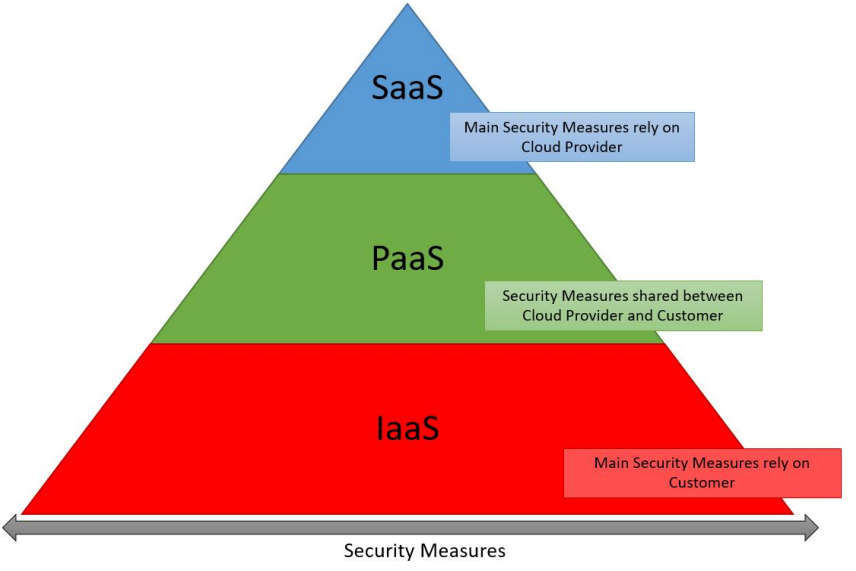

Abbildung 3: Cloud-Dienstmodelle und Sicherheitsverantwortung

a) IaaS

Der Cloud-Provider stellt dem Kunden eine oder mehrere virtuelle Maschinen zur Verfügung. Die gesamte Konfiguration und das Management der Anwendungen auf der (bereitgestellten) Infrastruktur bleiben im Verantwortlichkeitsbereich des Kunden. Daher ergeben sich die meisten Massnahmen in Bezug auf Vertraulichkeit und Integrität aus der Konfiguration durch den Kunden. Es ist jedoch zu beachten, dass der Cloud-Provider in technischer Hinsicht nach wie vor dafür verantwortlich ist, dass die auf den virtuellen Maschinen der Kunden gespeicherten Daten nicht von den virtuellen Maschinen

anderer Benutzer, einschliesslich des Providers selbst, abgerufen werden können (Vertraulichkeit) und dass diese Daten auf Anfrage des Berechtigten jederzeit verfügbar sind (Verfügbarkeit).

b) PaaS

Beim PaaS-Dienstmodell ist die Verantwortung für die Sicherheit geteilt, weil die Infrastruktur und die Plattform vom Cloud-Provider bereitgestellt werden und es dem Nutzer freisteht, die Umgebung in der Cloud nach seinen Anforderungen zu konfigurieren. Der Cloud-Provider ist dafür verantwortlich, dass die Kundendaten und -konfigurationen innerhalb der Infrastruktur vertraulich und jederzeit für den Kunden verfügbar sind. Der Kunde ist jedoch für die Konfiguration der Plattform und deren Sicherheitsaspekte verantwortlich.

c) SaaS

Im Gegensatz zu IaaS und PaaS hat der Nutzer beim SaaS-Dienstmodell eine lediglich minimale Sicherheitsverantwortung. In diesem Modell ist der Nutzer allein für die Sicherheit der Zugangsdaten verantwortlich. Die Vertraulichkeit der Daten, die Integrität des Netzwerks und die Verfügbarkeit der Dienste liegen in der alleinigen Verantwortung des Cloud-Providers.

3.2 Szenario 1

In Abbildung 4 werden zwei mögliche Implementierungen eines Cloud-Speichermodells dargestellt. In der oberen Hälfte der Abbildung wird die Speicherung der Daten nicht mehr lokal in der Anwaltskanzlei, sondern bei einem Cloud-Provider durchgeführt. Die Übertragung über das Netzwerk erfolgt dabei sicher – d.h. mit verschlüsselten Daten – unter Verwendung des HTTPS (Hypertext Transfer Protocol Secure)-Protokolls unter Ausnutzung von TLS (Transport Layer Security), das u.a. eine starke (128 Bit) oder noch stärkere (256 Bit) Schlüsselgrösse einsetzt. TLS ist die aktualisierte

Version von SSL (Secure Socket Layer) 3.0[1]. Jegliche Kommunikation, die auf HTTPS angewiesen ist, muss TLS als Verschlüsselungsprotokoll verwenden. Die Daten selbst erreichen den Cloud-Provider in IP (Internet-Protokoll)-Paketen, wobei sie vor der Übertragung verschlüsselt werden. Sobald der Cloud-Provider diese IP-Pakete in seiner lokalen Infrastruktur ablegt, werden die Daten mit einem lokalen Schlüssel des Cloud-Providers verschlüsselt, z.B. mit dem AES (Advanced Encryption Standard)-Verschlüsselungsverfahren.

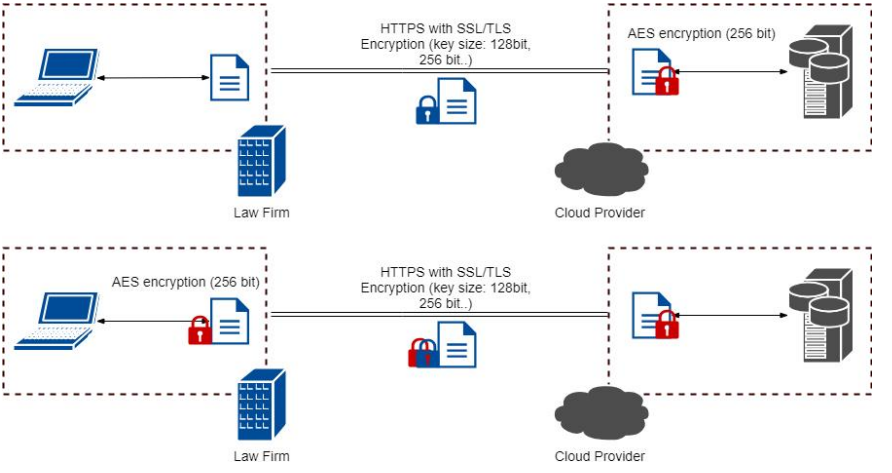

Abbildung 4: IaaS Cloud-basierte Speicherung mit alternativer Schlüssel-Verwaltung

Der untere Teil von Abbildung 4 zeigt, dass die beim Cloud-Provider zu speichernden Daten bereits vor der Übertragung über das Netzwerk von der Anwaltskanzlei verschlüsselt werden können. Damit hat lediglich die Anwaltskanzlei Zugang zu den Daten, weil nur sie über den erforderlichen Schlüssel verfügt. In diesem Fall vertraut die Anwaltskanzlei nicht auf die Verschlüsselung durch den Kommunikationsanbieter, sondern auf diejenige des Cloud-Providers, die sie aber selbst anwendet. Die verbleibenden Schritte für eine verschlüs-

[1] SSL 3.0 wurde von der IETF (Internet Engineering Task Force) im Dokument RFC 7568 als veraltet eingestuft.

selte Übertragung und die Speicherung auf Seiten des Cloud-Providers bleiben unverändert, mit der Ausnahme, dass der Cloud-Provider die Daten vor dem Speichern nicht mehr verschlüsseln muss. Während der Übertragung werden die Daten zweifach geschützt – mit dem Schlüssel der Anwaltskanzlei und mit dem angewendeten HTTPS SSL/TLS-Schlüssel.

Cloud-Computing – insb. auch die Cloud-basierte Speicherung von Daten («*Cloud Storage*») – bringt nicht nur Vorteile mit sich; die Kombination der verschiedenen Technologien eröffnet vielmehr auch neue Schwachstellen. So wurden z.B. die geläufigen Virtualisierungsmechanismen nicht speziell für das Cloud-Computing entwickelt, sondern lediglich an das Cloud-Computing *angepasst*, um die Nutzung der verfügbaren Ressourcen zu maximieren. Wie das herkömmliche Speichern und Bearbeiten von Daten, bspw. das Einschliessen von Dokumenten in einem Tresor oder das Bearbeiten und Speichern auf einem «*stand alone*»-Computer, ist auch die Nutzung von Cloud-Diensten mit gewissen Sicherheitsrisiken verbunden. Um diese Risiken zu minimieren sind spezifische Sicherheitsmassnahmen vorzusehen, welche je nach Angriffsmodell bzw. Risikoabwägung spezifisch auszuwählen sind.

3.3 Szenario 2

In dem in Abbildung 5 dargestellten Szenario 2 setzt eine Anwaltskanzlei Applikationen zur Textverarbeitung, Tabellenkalkulation oder zum Erstellen einer Präsentation in einem SaaS-Modell ein. In einem solchen Modell verwaltet der Cloud-Provider die Software für die Kanzlei in einer virtuellen Maschine («*hosting*»). Die Daten werden zwischen der Kanzlei und dem Cloud-Provider über HTTPS mit SSL/TLS verschlüsselt übertragen. Diese Daten sind jedoch keine Dateien oder Dokumente, wie in Szenario 1, sondern Informationen über die Aktionen des Nutzers in der Software (z.B. Kopieren, Einfügen, Editieren, neue Datei, Speichern). Das Dokument wird nach dem Speichern durch die Software vom Cloud-Provider mit einem für

jeden Nutzer unterschiedlichen Schlüssel verschlüsselt und archiviert. Zu beachten ist, dass in diesem SaaS-Modell der Cloud-Provider technisch gesehen über den Zugang zu den im Dokument gespeicherten Daten hat. Andere Cloud-Nutzer verfügen jedoch über keinen Zugang, weil die Dokumente mit unterschiedlichen Schlüsseln verschlüsselt wurden und so eine Datenisolierung gewährleistet ist. Die Inhalte der Dateien sind folglich für den Cloud-Provider sichtbar, nicht aber für andere Kunden desselben Cloud-Providers, welche diesen Dienst ebenfalls nutzen. Kunden, die mit vertraulichen Dateien zu tun haben, müssen sich bei der Verwendung von SaaS daher bewusst sein, dass der Cloud-Provider ihre Daten theoretisch verwenden kann. Die Dienste solcher Cloud-Provider sollten deswegen aus technischer Sicht mit entsprechender Zurückhaltung genutzt und es sollten adäquate Vorsichtsmassnahmen ergriffen werden.

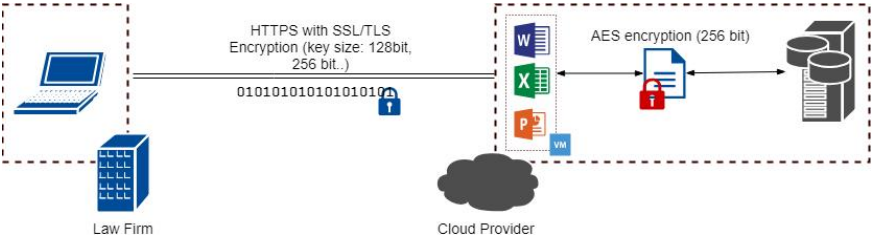

Abbildung 5: SaaS Cloud-Provider mit anbieterabhängigen Sicherheitsmechanismen

III. Strafrecht

Ob sich in der Schweiz tätige Anwältinnen und Anwälte strafbar machen, wenn sie bei der Ausübung ihres Berufes für das Bearbeiten von Daten die Dienste von Cloud-Providern nutzen, beurteilt sich in erster Linie nach dem Tatbestand der Verletzung des Berufsgeheimnisses (Art. 321 StGB). Der datenschutzrechtliche Straftatbestand der Verletzung der beruflichen Schweigepflicht (Art. 35 DSG) und die Regelung des Berufsgeheimnisses der Anwältinnen und Anwälte (Art. 13 BGFA) sind ergänzend heranzuziehen. Im Zentrum der strafrechtlichen Beurteilung steht die Frage, ob das Speichern und Bearbeiten von Daten in einer Cloud als strafrechtlich relevante Offenbarung eines Geheimnisses zu qualifizieren ist. Hierzu muss insb. geklärt werden, ob Cloud-Provider in strafrechtlicher Hinsicht als Hilfspersonen gelten und ob die Offenbarung an eine Hilfsperson den Tatbestand erfüllt.

1. Verletzung des Berufsgeheimnisses (Art. 321 StGB)

1.1 Deliktstypus

Die Strafbestimmungen des BT StGB werden in verschiedene Deliktstypen unterteilt, je nachdem, welche Elemente für den objektiven Tatbestand konstitutiv sind. Zunächst wird nach dem Zeitpunkt der Vollendung des objektiven Tatbestandes differenziert. Bei abstrakten Gefährdungsdelikten ist der Vollendungszeitpunkt am weitesten vorverlegt und tritt schon ein, wenn eine Handlung ausgeführt wird, die vom Gesetzgeber ganz generell – also abstrakt – als gefährlich eingestuft wird[2]. Bei konkreten Gefährdungsdelikten muss mindes-

[2] Beispiel: Wenn Pornografie zugänglich gemacht wird, ist der objektive Tatbestand von Art. 197 Abs. 1 StGB schon erfüllt, wenn der Abruf bzw. das Anschauen durch irgendeine Person unter 16 Jahren möglich ist. Etwa, wenn eine pornografische Datei auf eine öffentlich zugängliche Webseite abgespeichert wird. Der

tens ein Rechtsgutsträger oder-objekt nachweislich gefährdet werden. Daher genügt bei diesen Delikten die Ausführung der Tathandlung nicht. Zusätzlich muss eine konkrete Gefährdung für einen Rechtsgutsträger eintreten[3]. Die meisten Straftatbestände fordern mehr als eine Gefährdung des Rechtsguts bzw. des Rechtsgutsträgers. Zu ihrer Vollendung muss eine Verletzung vorliegen[4]. Eine weitere Differenzierung ordnet die Straftatbestände in (reine) Tätigkeits- und Erfolgsdelikte. Nach der strafrechtlichen Verbrechenslehre genügt es bei Tätigkeitsdelikten zur Vollendung, wenn die Tathandlung *ausgeführt* wird. Bei Erfolgsdelikten muss zusätzlich ein Erfolg eingetreten sein. Bei den genannten Unterscheidungsmerkmalen gibt es Überschneidungen, doch gelten alle abstrakten Gefährdungsdelikte als (schlichte) Tätigkeitsdelikte, weil das Delikt schon bei der blossen Ausführung der Handlung vollendet wird[5]. Bedeutung haben diese Unterscheidungen nicht nur mit Blick auf die Abgrenzung von Versuch und Vollendung sowie die objektiven Tatbestandselemente, die im Strafverfahren zu beweisen sind, sondern insb. auch für das Strafanwendungsrecht (siehe Art. 3 ff. StGB)[6].

Begriff des «abstrakten» Gefährdungsdelikts ist widersprüchlich, siehe SCHWARZENEGGER, sic! 2001, 247 m.w.H.

3 Beispiel: Wenn ein Täter einen Brief mit ehrenrührigen Beschuldigungen schreibt, ist der Tatbestand der üblen Nachrede oder der Verleumdung noch nicht vollendet. Es muss noch die Wahrnehmung eines beliebigen Dritten hinzutreten, damit der objektive Tatbestand vollendet wird (Art. 173 f. StGB). D.h., der Brief muss versandt und vom Empfänger gelesen werden. Erst in diesem Moment ist die Ehre des Beschuldigten konkret in Gefahr.

4 Beispiel: Es genügt nicht, einen Schuss auf eine Person abzufeuern (konkrete Gefährdung), sondern es muss der Tod des Opfers eintreten, damit der objektive Tatbestand der vorsätzlichen Tötung erfüllt ist (Art. 111 StGB).

5 Zu den Unterscheidungen im Kontext des Internet weiterführend: SCHWARZENEGGER, E-Commerce, 346 ff. m.w.H.

6 Das für die Strafhoheit in erster Linie massgebliche Territorialitätsprinzip knüpft bei reinen Tätigkeitsdelikten und abstrakten Gefährdungsdelikten nach h.L. nur am Handlungsort an (siehe hinten III.1.6).

Die Ausgestaltung von Art. 321 StGB als Antragsdelikt weist darauf hin, dass primär ein subjektives Recht des Geheimnisherrn geschützt wird[7]. Deutlich wird dies auch durch die Möglichkeit eines tatbestandsausschliessenden Einverständnisses bzw. einer rechtfertigenden Einwilligung[8] in Ziff. 2 indiziert. Das strafrechtliche Berufsgeheimnis erfasst aber nicht alle Verhältnisse zwischen einer Berufsgruppe und ihren Klienten, sondern nur jene, «bei denen ein öffentliches Interesse daran besteht, dass sich der Klient dem Berufsträger rückhaltlos anvertrauen kann»[9]. Insofern leitet sich die Strafnorm mittelbar auch aus dem öffentlichen Interesse am Schutz des besonderen Vertrauensverhältnisses ab, da erst durch die Vertraulichkeit der anwaltlichen Beziehung der Beruf richtig und einwandfrei ausgeübt werden kann[10]. Das ändert aber nichts daran, dass diese Strafbestimmung als Delikt gegen ein Individualrechtsgut konzipiert ist. Das öffentliche Interesse manifestiert sich allein in der Einschränkung auf die genannten Berufsgruppen[11].

Abstrakte Gefährdungsdelikte schützen Allgemeininteressen. Ihre Vollendung setzt schon bei der Tathandlung an (Vorfeldkriminalisie-

---

7 Das lässt sich schon den Materialien entnehmen: Expertenkommission I, Bd. 2, Bern 1896, S. 14 «Verletzung in den persönlichen Verhältnissen des Betroffenen»; ZÜRCHER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 364 «das private Geheimnis des Geheimnisinhabers» wird geschützt. Also nicht etwa das Recht des Geheimnisträgers, siehe NIGGLI, Gutachten Unternehmensjuristen, 17, 32 m.w.H. «Geheimsphäre des Berechtigten»; PK-StGB, TRECHSEL/VEST, StGB 321 N 1 m.w.H. das StGB hat sich «dieser Richtung angeschlossen».

8 Art. 321 Ziff. 2 StGB spricht von einer Einwilligung des Berechtigten. Im Gegensatz zur Einwilligung, die rechtfertigende Wirkung hat, spricht man von einem Einverständnis, wenn die Rechtswidrigkeit konstitutives Element der generell-abstrakten Unrechtsdefinition ist und das Einverständnis damit schon die Tatbestandsmässigkeit dahinfallen lässt. Bedeutung hat diese Unterscheidung insofern, als im letzteren Fall der Vorsatz auch die Rechtswidrigkeit erfassen muss. Am Beispiel der urheberstrafrechtlichen Bestimmungen SCHWARZENEGGER, ZSR 2008 II, 467 m.w.H.

9 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 4.

10 BGE 112 Ib 606, E. b. Vgl. PK-StGB, TRECHSEL/VEST, StGB 321 N 1 m.w.H.

11 Ebenso NIGGLI, Gutachten Unternehmensjuristen, 32 m.w.H.

rung), zu einem Zeitpunkt also, in welchem ein individualisierbarer Rechtsgutsträger gar noch nicht feststellbar ist. Sie sind daher Offizialdelikte[12]. Daraus folgt, dass Art. 321 Ziff. 1 Abs. 1 StGB kein abstraktes Gefährdungsdelikt sein kann. Nach der Rechtsprechung des Bundesgerichts und der h.L. wird die Kenntnisnahme durch einen Dritten für die Vollendung der Tat vorausgesetzt[13]. Das bedeutet, dass eine Verletzung des materiellen Geheimnisses Voraussetzung für die Verwirklichung des objektiven Tatbestandes ist. Diese Charakterisierung passt allerdings nicht zur häufig wiederholten Formel, die Tathandlung sei erfüllt, wenn der Täter das Geheimnis einer dazu nicht ermächtigten Drittperson zur Kenntnis bringe oder «dieser die Kenntnisnahme zumindest ermögliche»[14]. Auch kann der Tatbestand dann nicht schon durch eine unzureichende Aufbewahrung der geheimen Informationen vollendet werden[15]. Folgt man der h.L., dann ist Art. 321 Ziff. 1 Abs. 1 StGB ein Verletzungsdelikt. Sobald eine Person, die Geheimnisträger im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB ist, durch ein Tun oder Unterlassen kausal bewirkt, dass mindestens ein unbefugter Dritter vom Geheimnis Kenntnis nimmt, ist der objektive

---

12 SCHMID, § 5 N 11 m.N.; SCHWARZENEGGER, ZSR 2008 II, 464 f.

13 BGer 6B_1403/2017, Urteil vom 8. August 2017, E. 1.2.2; ISENRING, StGB/JStGB-Kommentar, StGB 321 N 10b; DONATSCH/THOMMEN/WOHLERS, 580 f.; BSK-Strafrecht II, NIGGLI/HAGENSTEIN, StGB 162 N 36; BSK-Strafrecht II, OBERHOLZER, StGB 320 N 10.

14 BGE 142 IV 65, E. 5.1; BSK-Strafrecht II, OBERHOLZER, StGB 320 N 10; BGer 6B_1403/2017, Urteil vom 8. August 2017, E. 1.2.2, meint dazu: «Es handelt sich hierbei um eine blosse Umschreibung des strafbaren Verhaltens, woraus – entgegen der Meinung der Vorinstanz – nichts zum Zeitpunkt der Vollendung der Tat abgeleitet werden kann. Vielmehr ist in dieser Frage der Lehre zu folgen, wonach die Tat vollendet ist, sobald ein Aussenstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält». Diese Begründung ist eine *Petitio Principii* und überzeugt nicht.

15 So aber BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; STRATENWERTH/BOMMER, § 61 N 19; PK-StGB, TRECHSEL/VEST, StGB 321 N 23, was eher für ein konkretes Gefährdungsdelikt sprechen würde. Wenn zur Vollendung mindestens die Kenntnisnahme eines unbefugten Dritten vorliegen muss, dann ist die unzureichende Aufbewahrung per se höchstens als Versuch der Berufsgeheimnisverletzung strafbar.

Tatbestand von Art. 321 Ziff. 1 Abs. 1 StGB vollendet[16]. Da die Kenntnisnahme des Geheimnisses eine von der Tathandlung verursachte, separate Aussenwirkung darstellt, handelt es sich bei Art. 321 Ziff. 1 Abs. 1 StGB zugleich um ein Erfolgsdelikt.

Zusammenfassend lässt sich festhalten, dass Art. 321 StGB zu den Delikten gegen Individualrechtsgüter zählt. Es handelt sich gleichzeitig um ein Verletzungs- und Erfolgsdelikt.

1.2 Objektiver Tatbestand

a) Angriffsobjekt: Das geschützte Geheimnis

Angriffsobjekt bei einer Berufsgeheimnisverletzung ist ein Geheimnis, das dem Täter infolge des Berufes anvertraut oder von ihm in dessen Ausübung wahrgenommen wurde. Rechtlichen Schutz geniessen materielle Geheimnisse. Ein Geheimnis muss danach relativ unbekannt sein und der Geheimnisherr muss ein berechtigtes Interesse an der Geheimhaltung der Information haben[17].

i. Relative Unbekanntheit

Relative Unbekanntheit ist gegeben, wenn nur eine beschränkte Anzahl von Personen über die fraglichen Informationen verfügt. Die tatsächliche Kenntnis einer Drittperson ist daher nicht entscheidend. Unter den Schutz des Berufsgeheimnisses fällt auch eine Information, die der Empfänger bereits hat oder vermutet, weil dadurch seine un-

---

16 So schon GAUTIER, Expertenkommission II, Bd. IV, Luzern 1915, S. 365 «*consommé par la révélation*».

17 BGE 127 IV 122, E. 1; 142 IV 65, E. 5.1 je m.w.H. (zu Art. 320 StGB); NIGGLI, Gutachten Unternehmensjuristen, 20 ff. m.w.H; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 14; STRATENWERTH/BOMMER, § 61 N 5; PK-StGB, TRECHSEL/VEST, StGB 321 N 20 ff. m.w.H.

sicheren oder unvollständigen Kenntnisse ergänzt oder verstärkt werden[18].

ii. Materielles Geheimnis

Beim materiellen Geheimnisbegriff steht das Interesse des Geheimnisherrn im Vordergrund[19]. Der Geheimnisherr soll – auch wenn er über geheime Tatsachen mit einem Anwalt oder einem anderen in Art. 321 Ziff. 1 Abs. 1 StGB genannten Berufsangehörigen spricht – die Kontrolle über die Offenbarung der Information an Dritte behalten. Das Berufsgeheimnis schafft damit ein Vertrauensverhältnis, das es dem Anwalt ermöglichen soll, den Sachverhalt umfassend abzuklären, den Klienten richtig zu beraten und ihm den Zugang zum Recht zu verschaffen[20]. Nicht unter das Berufsgeheimnis gemäss Art. 321 Ziff. 1 Abs. 1 StGB fallen Informationen aus der sog. akzessorischen anwaltlichen Geschäftstätigkeit, also aus der Vermögensverwaltung, aus Depotgeschäften, Inkassomandaten und Verwaltungsratsmandaten[21], oder aus dem Privatleben des Anwalts.

Art. 321 StGB erfasst alle Informationen, die dem Anwalt infolge seines Berufes anvertraut wurden, sowie alle Informationen, die er bei dessen Ausübung wahrgenommen hat. Art. 321 StGB enthält keine Beschränkung auf Informationen bezüglich des Klienten und verlangt

---

18 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19 STRATENWERTH/BOMMER, § 61 N 7; BGE 75 IV 71, E. 1; FELLMANN, Rn. 542.

19 NIGGLI, AwR 2006, 279 m.w.H.; STRATENWERTH/BOMMER, § 61 N 5, 15; DONATSCH/THOMMEN/WOHLERS, 587; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 1; so schon ZÜRCHER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 364.

20 Vgl. BSK-Strafrecht II, OBERHOLZER, StGB 321 N 2; WOHLERS/LYNN, recht 2018, 12.

21 Vgl. BGE 143 IV 462, E. 2.2; NIGGLI, Gutachten Unternehmensjuristen, 21 ff.; PK-StGB, TRECHSEL/VEST, StGB 321 321 N 21. Strafrechtlichen Schutz soll nur die anwaltstypische Tätigkeit geniessen, wobei die Abgrenzungen in der Praxis schwierig sind (siehe zur Auslagerung von GwG-Compliance Aufgaben an eine Anwaltskanzlei: BGer 1B_85/2016, Urteil vom 20. September 2016, E. 6).

umgekehrt auch nicht, dass die Information dem Anwalt bewusst mitgeteilt oder übergeben wurde[22]. Die Geheimnisse können somit auch von Dritten stammen, die diesbezüglich Geheimnisherren sind. Entscheidend ist lediglich ein Kausalzusammenhang zur Mandatsausübung[23].

Im Rahmen dieses Gutachtens ist die Geheimnisqualität nicht weiter zu untersuchen. Unbestrittenermassen sind beim Outsourcing von Klientendaten Berufsgeheimnisse tangiert.

b) Täterkreis: Geheimnisherr und Hilfspersonen

Art. 321 StGB ist ein echtes Sonderdelikt, d.h. taugliche Täter sind nur die explizit und abschliessend aufgezählten Berufsangehörigen[24]. Anwälte und Anwältinnen, aber auch ihre Hilfspersonen werden in der Bestimmung namentlich erwähnt und können sich daher nach Art. 321 Ziff. 1 Abs. 1 StGB strafbar machen[25]. Zur Kategorie der Anwälte zählen alle Personen, die eine entsprechende fachliche Ausbildung abgeschlossen haben und über einen schweizerischen oder ausländischen Fähigkeitsausweis verfügen, wobei es keine Rolle spielt, ob sie im anwaltschaftlichen Monopolbereich tätig sind oder nicht[26]. Auch auf den Eintrag im kantonalen Anwaltsregister kommt es nicht an. Strittig ist, ob das Anwaltsgeheimnis nur für den unabhängigen

---

22 So schon GAUTIER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 365; NIGGLI, AwR 2006, 279; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 16; PK-StGB, TRECHSEL/VEST, StGB 321 N 21 f.

23 Vgl. BGE 115 Ia 197, E. 3.c, gemäss dem die Geheimhaltungspflicht des Anwalts bzw. der Anwältin nur Tatsachen betrifft, die ihm oder ihr von Klienten anvertraut worden sind, um die Ausübung des Mandats zu ermöglichen, oder die in Ausübung des Mandats wahrgenommen wurden (ebenso BGE 112 Ib 606, E. b). FELLMANN, Rn. 559 f.

24 ZÜRCHER, 351; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 11; PK-StGB, TRECHSEL/VEST, StGB 321 N 3; STRATENWERTH/BOMMER, § 61 N 17.

25 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 4; PK-StGB, TRECHSEL/VEST, StGB 321 N 5; BOHNET/MARTENET, 741.

26 NIGGLI, Gutachten Unternehmensjuristen, 15, 19 f.

und selbständigen Anwalt oder auch für Unternehmensjuristen gilt[27]. Da die Verteidigung von beschuldigten Personen gemäss StPO Anwälten vorbehalten ist, die nach dem BGFA berechtigt sind, Parteien vor Gerichtsbehörden zu vertreten (Art. 2 BGFA, Art. 127 Abs. 5 StPO, Ausnahme: Verteidigung in Übertretungsstrafverfahren), hat die zusätzliche Erwähnung von Verteidigern in Art. 321 Ziff. 1 Abs. 1 StGB kaum mehr eigenständige Bedeutung. Von der Norm sind auch Notare und Patentanwälte sowie weitere Berufsgruppen erfasst[28].

Für die vorliegende Fragestellung entscheidend ist die Auslegung des Begriffes der Hilfsperson eines zur Geheimhaltung verpflichteten Berufsangehörigen. Als Hilfspersonen werden in Lehre und Rechtsprechung genannt[29]: Assistenten, Sekretäre, externe Schreibbüros («ausgelagertes Sekretariat»)[30], Kanzleipersonal, Praktikanten, Buchhalter, Privatdetektive[31], Experten, alle Mitarbeiter im unter ärztlicher Leitung stehenden Team (Psychologen, Pädagogen, Sozialarbeiter, Pfleger, Therapeuten, Laborpersonal), Krankenpflegepersonal, Arztgehilfen, untergeordnetes Hilfspersonal, soweit es mit Patienteninformationen in Berührung kommt, Zahntechniker[32], Hebammen (falls sie unter Anleitung eines Arztes handeln[33]) sowie Reinigungs-

---

27 Vgl. BSK-Strafrecht II, OBERHOLZER, StGB 321 N 6; PK-StGB, TRECHSEL/VEST, StGB 321 N 5 welche die Unternehmensjuristen für nicht erfasst betrachten; weiterführend zur Kontroverse NIGGLI, Gutachten Unternehmensjuristen, *passim*; PFEIFER, AwR 2006, 166 ff.; NIGGLI, AwR 2006, 277 ff.

28 Zu den einzelnen Berufsgruppen näher BSK-Strafrecht II, OBERHOLZER, StGB 321 N 5 ff.; PK-StGB, TRECHSEL/VEST, StGB 321 N 6 ff.

29 BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.3; BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 10; DONATSCH/THOMMEN/WOHLERS, 590; KELLER, 107; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 10; STOCKER, ZStrR 1953, 9; PK-StGB, TRECHSEL/VEST, StGB 321 N 13; s.a. BGer 1B_447/2015, Urteil vom 25. April 2016, E. 2.2.

30 BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.5.

31 BGer 1B_447/2015, Urteil vom 25. April 2016, E. 2.2; CORBOZ, CP 321 N 16; FELLMANN, Rn. 555; CR-LLCA, MAURER/GROSS, LLCA 13 N 97.

32 PK-StGB, TRECHSEL/VEST, StGB 321 N 10.

33 PK-StGB, TRECHSEL/VEST, StGB 321 N 12.

personal und Personal in der Telefonzentrale, soweit sie mit Informationen über den Geheimnisherrn in Berührung kommen[34].

Nach einigen Autoren soll das Wartungspersonal für technische Einrichtungen nicht als Hilfsperson im Sinn von Art. 321 StGB qualifiziert werden können[35]. Das kann in dieser Allgemeinheit nicht richtig sein. Vielmehr ist wie beim Reinigungspersonal danach zu unterscheiden, ob das Wartungspersonal in selber Funktion Kenntnis von Informationen über die Klienten des Anwalts erhält. Wenn es um den Betrieb einer Heizung in der Anwaltskanzlei geht, ist keine Hilfspersonenstellung anzunehmen, weil der Hauswart nicht mit der Bearbeitung von Dokumenten betraut wird. Hingegen sind IT-Spezialisten, die im Auftrags- oder Anstellungsverhältnis den Anwalt bei der Dokumentenverwaltung und -archivierung sowie der Software-Bedienung unterstützen sollen, eindeutig in einem Bereich tätig, in dem die Kenntnisnahme von Geheimnissen unvermeidlich ist[36]. Im Gegensatz zu früher, als die Dokumentenverwaltung in Papierform erfolgte, ist heute der IT-Support eine der zentralen Hilfsfunktionen bei der digitalen Informationsverarbeitung und Dokumentenverwaltung, so auch in der Anwaltskanzlei. Der IT-Spezialist bzw. die Mitarbeitenden des IT-Providers, die mit Arbeiten im Zusammenhang mit IT-Infrastruktur und Applikationen betraut sind, gehören folglich zur Kategorie der Hilfspersonen[37].

---

34 PK-StGB, TRECHSEL/VEST, StGB 321 N 13; REHBERG, 340 f. Bezüglich dieser Kategorie a.M. STRATENWERTH/BOMMER, § 61 N 17, was nicht überzeugt. Wird das Putzpersonal zu den unbefugten Dritten gezählt, muss der Anwalt bzw. die Anwältin vom Geheimnisherrn vorgängig eine Einwilligung einholen, d.h. bevor er oder sie die Büroräumlichkeiten putzen lässt, oder aber er oder sie muss selber putzen, um das Strafbarkeitsrisiko nach Art. 321 StGB auszuräumen.

35 PK-StGB, TRECHSEL/VEST, StGB 321 N 13 m.w.H. auf LANGMACK, ZStrR 1972, 67; ROSSEL, SZS 1992, 243 f., wo es jeweils um Hilfspersonen von Ärzten geht.

36 So auch für interne IT-Mitarbeitende WOHLERS, 23.

37 Ähnlich bezüglich der arbeitsteiligen internen Organisation in Banken (mit Blick auf Art. 47 BankG), ALTHAUS STÄMPFLI, 143, welche die «Informatik» explizit als

Wer Hilfsperson im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB ist, hat die gleiche Pflicht zur Geheimhaltung der Informationen, die ihr im Zusammenhang mit der Tätigkeit für den (Haupt-)Geheimnisträger anvertraut werden oder von denen sie dabei Kenntnis erhält, wie der (Haupt-)Geheimnisträger selbst. Daraus ergeben sich gestützt auf eine grammatikalische, systematische, historische und teleologische Auslegung des Gesetzes zwei wichtige Schlussfolgerungen (i und ii). Ausserdem ist auf arbeitsteilige Organisationsformen näher einzugehen, bei denen mehrere (Haupt-)Geheimnisträger nebeneinander aktiv sind (iii).

i. Funktionale Definition der Hilfsperson

Nach der grammatikalischen Auslegung, die am Wortsinn ansetzt, sind Hilfspersonen (franz. «*auxiliaires*», ital. «*ausiliari*») Individuen, die jemanden bei der Erfüllung einer Aufgabe unterstützen. Der Wortsinn erfasst alle möglichen Hilfstätigkeiten, seien es Schreibarbeiten, Recherchen, Botengänge oder die Unterstützung bei der Datenerfassung, -bearbeitung und -archivierung. Auch Outsourcingnehmer, die für den Geheimnisträger eine effiziente Datenverarbeitung bereitstellen, können ohne weiteres unter diesen Begriff gefasst werden.

Die systematische Auslegungsregel erschliesst die Bedeutung einer Norm aus dem Zusammenhang mit anderen Normen und Gesetzen. Auch innerhalb einer Bestimmung können sich Hinweise für die Auslegung ergeben, so etwa bei Aufzählungen, die den Täterkreis oder die möglichen Tathandlungen charakterisieren. Dass die Hilfspersonen in Art. 321 Ziff. 1 Abs. 1 StGB in einem Atemzug mit den Kategorien der (Haupt-)Geheimnisträger genannt (dt. «sowie …», franz. «*ainsi que* …», ital. «*come pure* …») und der gleichen Strafdrohung unterworfen werden, ist ein starkes Indiz dafür, dass der Gesetzgeber

«Personen, welche einen Beitrag an die vom Kunden gewünschten Dienstleistungen erbringen», aufführt.

den Kreis der Personen, die das Geheimnis zur Kenntnis nehmen, breiter fassen wollte, weil er von einer funktionalen arbeitsteiligen Umgebung ausging. Hätte er den Kreis der Hilfspersonen enger fassen wollen, hätte sich das begrifflich niederschlagen müssen.

Klare Hinweise ergeben sich auch aus der historischen Auslegung. Der Gesetzgeber ging davon aus, dass Geistliche, Anwälte, Verteidiger, Notare, Patentanwälte usw. ihre Berufstätigkeit nicht völlig alleine ausüben müssen, sondern arbeitsteilig handeln dürfen[38]. Die Gesetzesmaterialien verdeutlichen, dass die Auffassung, man müsse den Kreis der Hilfspersonen eng eingrenzen, explizit abgelehnt wurde. Die Zweifel zweier Mitglieder der Expertenkommission, die eine engere Begriffsfassung befürworteten, wurden zur Kenntnis genommen, aber bewusst nicht berücksichtigt. So wies ALFRED GAUTIER in der zweiten Expertenkommission auf Abgrenzungsprobleme hin: «*Car il est délicat de délimiter le cercle de ces auxiliaires. On risque d'y comprendre de simples petits comparses sur lesquels ne doit reposer aucune responsabilité spéciale, …*»[39]. Die Expertenkommission ging auf dieses Argument nicht näher ein. Im Einklang mit GAUTIER stellte EUGÈNE DESCHENAUX einen Antrag, der eine Änderung des Begriffs «*auxiliaire*» in «*assistant ou employé supérieur*» verlangte[40]. Damit verband sich eine sehr restriktive Vorstellung darüber, wie das Geheimnis in einem Büro gewahrt werden sollte: «*… ou bien le patron met sous clef ce qui doit rester secret, ou bien c'est lui qui encourt la responsabilité pour ne s'être pas entouré d'un personnel suffisamment discret et réservé*»[41]. Der Chef müsse also alles persönlich einschliessen, wenn er sicher gehen wolle. Der Antrag DESCHENAUX wurde von der Expertenkommission mit

[38] PK-StGB, TRECHSEL/VEST, StGB 321 N 23 zur Arbeitsteilung in Teams; auch WOHLERS, 21, anerkennt die Notwendigkeit der Arbeitsteilung grundsätzlich.

[39] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 365.

[40] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 371. Es ging ihm v.a. darum, die untergeordneten Angestellten aus einer möglichen Strafbarkeit auszunehmen.

[41] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 372.

grosser Mehrheit abgelehnt[42]. Auch in der parlamentarischen Beratung des Gesetzes führte der Hinweis des Kommissionspräsidenten des Nationalrates, die Bezeichnung «Gehilfen solcher Personen» sei etwas vage, zu keiner Diskussion oder Einengung des Begriffsverständnisses oder gar zu einer Anpassung der Strafbestimmung[43].

Auch aus teleologischer Sicht macht es keinen Sinn, den Kreis der Hilfspersonen eng zu begrenzen. In einer arbeitsteiligen Büroumgebung würde sich damit die Anzahl der unberechtigten Dritten automatisch erhöhen. Ob nun die Geheimnisse in Papierform oder als digitale Daten in einem lokalen Desktop-Computer, auf einem Netzwerkserver der Anwaltskanzlei oder aber in einer Cloud bearbeitet und abgelegt werden, in allen diesen Kontexten müsste der Geheimnisträger[44] bei einer engen Begriffsdefinition alles selber abschliessen, verschlüsseln, die IT-Betriebssysteme selber warten und die Datenverwaltung selbst managen, damit keine Möglichkeit des Zugriffs von unberechtigten Dritten – wie bspw. Putzpersonal, Sekretariat oder IT-Mitarbeiter – besteht. Es kann aber nicht Sinn und Zweck des Gesetzes sein, hochqualifizierte Berufsgruppen mit solchen Aufgaben zu belasten und betrieblich unmögliche oder zumindest höchst ineffiziente Prozesse zu fordern. Der Schutz des Geheimnisses und die Wahrung der Interessen des Geheimnisherrn werden vielmehr durch die Unterstellung der Hilfspersonen unter das Berufsgeheimnis und die zivil- und aufsichtsrechtliche Verantwortlichkeit des (Haupt-)Geheimnisträgers hinreichend gewährleistet. Dieser ist denn auch für eine sorgfältige Auswahl und Instruktion der Hilfspersonen verantwortlich.

Die verschiedenen Auslegungsansätze kommen zu einem klaren, übereinstimmenden Resultat: Der schweizerische Berufsgeheimnis-

---

42 Protokoll der zweiten Expertenkommission Strafgesetzbuch, 376.

43 Stenographisches Bulletin, Nationalrat, 26.9.1929, S. 612. Abweichend, ohne eigenständige Auslegung oder Berücksichtigung der Materialien SCHÄFER, 39 f.

44 Sowie die wenigen, als Hilfspersonen anerkannten Mitarbeitenden wie z.B. Praktikanten.

schutz folgt einem breit gefassten, funktionalen Verständnis der Hilfsperson[45]. Hilfsperson ist damit, wer bei der Berufstätigkeit eines (Haupt-)Geheimnisträgers in der Weise mitwirkt, dass er grundsätzlich von Geheimnissen Kenntnis erhalten kann. Es reicht, wenn die Hilfsperson den primär Verpflichteten bei der Erfüllung seiner Aufgaben unterstützt[46]. Der Umgang mit geheimen Informationen kann an Hilfspersonen übertragen werden, soweit nicht andere gesetzliche Vorschriften entgegenstehen. Das Berufsgeheimnis nach Art. 321 Ziff. 1 Abs. 1 StGB steht einer betriebswirtschaftlich sinnvollen Organisation der Arbeit von Berufsgeheimnisträgern nicht entgegen. Herkömmliche Tätigkeiten wie Sekretariatsarbeiten, Recherchen, Aktenführung und –archivierung, Materialbeschaffung und -installation, Botengänge zur Post usw. können an Hilfspersonen übertragen werden. Das Gleiche muss für die elektronische Datenverarbeitung gelten. Die Installation und Wartung von Computern und Programmen, die elektronische Erfassung, Verarbeitung und Archivierung von Daten, die Fernwartung der Nutzergeräte usw. können faktisch nicht vom Geheimnisträger alleine bewältigt werden. Er benötigt dazu die Unterstützung von Spezialisten[47], die gemäss seinen Anweisungen und seiner Kontrolle tätig werden. Auch wenn man beim Berufsgeheimnis

---

45 BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.2, «Der Kreis der Hilfspersonen ist praktisch unbegrenzt»; CHAPPUIS/ALBERINI, AwR 2017, 339 f.; KELLER, 106 ff. m.w.H., mit der Einschränkung auf «Berufsmässigkeit»; NIGGLI, Gutachten Unternehmensjuristen 30 f.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 10; PK-StGB, TRECHSEL/VEST, StGB 321 N 13; STRATENWERTH/BOMMER, § 61 N 17, mit der Einschränkung auf «Berufsmässigkeit»;. Vgl. NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 51 f. und N 53: «Massgeblich ist vielmehr sowohl strafrechtlich als auch berufsrechtlich, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu geschützten Informationen einschliesst».

46 A.M., allerdings ohne eigenständige Auslegung oder Berücksichtigung der Materialien SCHÄFER, 39 f.; siehe auch HAFTER, 854 f. A.M. auch WOHLERS, siehe dazu III.1.2b)iv.

47 Siehe aus vertragsrechtlicher Sicht STRAUB, AJP 2014, 913: «Wenn der Auftraggeber selbst nicht über die entsprechenden Kompetenzen verfügt, kann die Datensicherheit eine Auslagerung der Datenbearbeitung an externe Spezialisten unter Umständen sogar erforderlich machen».

zunächst an den Schutz innerhalb der Büroräumlichkeiten des Geheimnisträgers denkt – in Analogie zum besonders gesicherten Büro und Archiv im Keller[48] –, sind Handlungen ausserhalb dieses geschützten Raums[49], ja sogar im Ausland[50], seit jeher möglich und miterfasst, so z.B. beim Absenden und der Entgegennahme der Post, bei auswärtigen Einvernahmen und Klientengesprächen, bei der Mitnahme geschützter Informationen als Kopie auf Papier oder auf einer Festplatte oder einem Memory-Stick, usw. Auch Hilfspersonen können dem Berufsgeheimnis unterstehende Informationen ausserhalb der Büroräumlichkeiten des Geheimnisträgers verwenden[51]. Sie müs-

---

48 Die in der Literatur diskutierten Konstellationen sind immer noch stark von der Vorstellung geprägt, dass Anwälte lediglich mit physischen Papierakten arbeiten. Eine unterschiedliche Behandlung von physischen und digitalen Prozessen würde sich dann aufdrängen, wenn die Digitalisierung zu fundamentalen Verschiebungen führen würde. Dies ist partout nicht der Fall, denn so führt z.B. das digitale Abspeichern passwortgeschützter Geheimnisse dazu, dass sie Dritten trotz Zutritts zu den Räumlichkeiten (z.B. dem Putzpersonal oder dem Heizungstechniker) unzugänglich sind.

49 Explizit BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.4.

50 Explizit BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.5, für in Deutschland ausgeführte Schreibarbeiten; A.M. bezüglich Handlungen im Ausland SCHWANINGER/LATTMANN, Jusletter 11. März 2013, Rn. 31, da die Strafrechtsdurchsetzung bei ausländischen Anbietern nicht gleich effektiv sei. Dem ist entgegenzuhalten, dass Fragen der Strafhoheit oder gar der Strafrechtsdurchsetzung keine Relevanz für die Tatbestandsmässigkeit nach Art. 321 Ziff. 1 Abs. 1 StGB haben (siehe dazu hinten, III.1.6). Hingegen setzt das Datenschutzrecht der Datenverarbeitung im Ausland bestimmte Grenzen (siehe dazu hinten, IV.3.1e)).

51 Man denke nur an die Tätigkeit eines Privatdetektivs, der zu den Hilfspersonen gezählt wird, siehe BGer 1B_447/2015, Urteil vom 25. April 2016, E. 2.2. Ebenso ein Urteil des BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.2, ein Psychiater hatte seinen Befund auf Band diktiert und das Material an ein externes Schreibbüro übermittelt, welches das Diktat transkribierte. Die Anklageschrift warf dem Psychiater vor, er habe es versäumt, für die Weitergabe des Krankenberichts die Zustimmung des Patienten einzuholen, obwohl er gesetzlich dazu verpflichtet gewesen wäre. Das Bezirksgericht Zürich hielt fest, dass die ausführenden Mitarbeiter des Schreibbüros Hilfspersonen des Arztes seien. Diese unterstünden der gleichen Geheimhaltungspflicht wie auch die Angestellten von Arztpraxen und Spitälern. Deshalb habe der Psychiater mit der Nutzung des ex-

sen dabei weder vom Geheimnisträger angestellt sein, noch muss die Tätigkeit auf Dauer oder entgeltlich sein[52]. Hingegen muss die Hilfsperson den (Haupt-)Geheimnisträger in seinem beruflichen Wirkungskreis unmittelbar unterstützen[53].

ii. Keine Offenbarung an Hilfspersonen

Gegenüber ihrer Hilfsperson können Geheimnisträger kein Geheimnis offenbaren, denn die Hilfspersonen gehören zum inneren Kreis der arbeitsteiligen Organisation des Geheimnisträgers. Sie werden mit anderen Worten Teil der gleichen Verantwortungssphäre, in welcher sich die Beteiligten gegenseitig vertrauen können müssen[54]. Beim Umgang mit geheimen Informationen in der Zusammenarbeit zwischen (Haupt-)Geheimnisträger und Hilfsperson kann der objektive Tatbestand von Art. 321 Ziff. 1 Abs. 1 StGB von vornherein nicht erfüllt werden[55]. Ausserhalb der gemeinsamen Verantwortungssphäre gilt demgegenüber der Geheimnisschutz gegenüber allen unbefugten Dritten. Hilfspersonen unterstehen daher wie der (Haupt-)Geheimnisträger der gleichen Strafdrohung.

iii. Nebeneinander von (Haupt-)Geheimnisträgern

Für bestimmte arbeitsteilige Organisationsstrukturen – zu denken ist insb. an ein behandelndes Team von Ärzten und Ärztinnen in einem

---

ternen Dienstleistungsangebots auch seine Pflicht zur Geheimhaltung nicht verletzt. Vgl. dazu auch FISCHER, 11.

52 BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.2 m.w.H.; A.M. WOHLERS, 26, der mit Hinweisen auf die Rechtslage in Deutschland zu § 203 a.F. D-StGB meint, eine Auslagerung an externe Dritte sei nicht über die Hilfspersonenzuordnung zu lösen, sondern höchstens über das Vorliegen eines Rechtfertigungsgrundes.

53 DONATSCH/THOMMEN/WOHLERS, 590; KELLER, 107 f. m.w.H.

54 PK-StGB, TRECHSEL/VEST, StGB 321 N 25; Siehe dazu auch die zivilrechtliche Regelung betreffend Haftung für Handlungen der Hilfsperson, Art. 101 OR; BSK-OR-I, WIEGAND, OR 101 N 4 f. So auch BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.3.

55 Explizit: BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.3.

Spital – ist es anerkannt, dass es auch zu einem Nebeneinander von (Haupt-)Geheimnisträgern kommen kann[56]. So z.B. wenn Ärzte verschiedener Fachrichtungen oder Ärzte mit unterschiedlichem Wissens- und Erfahrungsstand in die Behandlung eines Patienten miteinbezogen werden. Auch in diesen Konstellationen ist ein Offenbaren im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB nicht möglich[57]. Jeden einzelnen beteiligten Berufsgeheimnisträger trifft dafür die Pflicht, das Berufsgeheimnis zu wahren. Diese Art des Einbezugs weiterer Ärzte und sonstiger Personen und ihres Umgangs mit den geheimen Informationen sollte idealerweise schon im Behandlungsvertrag vorgesehen sein, allenfalls kann vom stillschweigenden Einverständnis des Patienten ausgegangen werden[58]. Diese Ausführungen gelten *mutatis mutandis* auch für ein Team von Anwälten und Anwältinnen, die einen komplexen Rechtsfall gemeinsam lösen.

iv. Position Wohlers zur Hilfsperson

WOLFGANG WOHLERS vertritt in seinem Gutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich in zwei wesentlichen

[56] BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; WOHLERS, 19 und 26, übernimmt aus dem deutschen Schrifttum den Begriff «Funktionseinheit», übersieht dabei aber, dass im schweizerischen Strafrecht die Figur der Hilfsperson ebenfalls funktional definiert wird (siehe vorn, III.1.2b)i). Der einzige Unterschied zwischen arbeitsteiligen Organisationsstrukturen und der funktionalen Aufgabenteilung zwischen (Haupt-)Geheimnisträger und Hilfsperson ist darin zu sehen, dass bei ersteren der Geheimnisherr sein Geheimnis von vornherein allen im Team tätig werdenden Geheimnisträgern anvertraut bzw. sich dies aus dem privatrechtlichen Verhältnis so ergibt. Der Unterschied ist bloss graduell.

[57] DONATSCH/THOMMEN/WOHLERS, 593; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; PK-StGB, TRECHSEL/VEST, StGB 321 N 23; enger WOHLERS, 19 gestützt auf Literatur zu § 203 a.F. D-StGB und unter Hinweis auf den «Kreis der zum Wissen Berufenen».

[58] KELLER, 114 ff.

Punkten abweichende Meinungen, die sich vor allem auf Quellen zum alten deutschen Recht (§ 203 a.F. D-StGB) stützen[59].

(i) Zum einen bestreitet WOHLERS das vorn (ii) festgestellte Resultat, dass ein (Haupt-)Geheimnisträger gegenüber einer Hilfsperson kein Geheimnis offenbaren könne und damit schon die Tatbestandsmässigkeit dahinfalle: «Hinzuweisen ist (…) an dieser Stelle darauf, dass die Einbeziehung der Hilfspersonen in den Kreis der Schweigepflichtigen nicht bedeutet, dass die Weitergabe des Geheimnisses an sie per se als straflos anzusehen ist. Ein derartiger Schluss liesse sich mit dem allgemein anerkannten Grundsatz nicht vereinbaren, dass auch die

[59] Das Gutachten trennt in den Belegen leider nicht immer zwischen der schweizerischen Literatur und den zu Art. 321 StGB entwickelten Auslegungsansätzen einerseits, sowie dem deutschen Schrifttum, das rechtsvergleichend beigezogen wurde. So stützt WOHLERS seine Standpunkte mehrfach auf Quellen, die sich auf § 203 a.F. D-StGB beziehen. § 203 a.F. D-StGB wies zwar Ähnlichkeiten mit Art. 321 StGB auf, doch existierten auch wesentliche Unterschiede. So fehlt das Antragserfordernis in § 203 a.F. D-StGB, erfasst die Norm in Abs. 2 auch Amtsträger und war insb. die Rolle der «Hilfspersonen» im deutschen Strafrecht anders gefasst («berufsmässig tätige Gehilfen», vgl. § 203 Abs. 3 Satz 2 a.F. D-StGB). Nach h.L. war in Deutschland ein externer Dritter, der für einen Geheimnisträger im Sinn von § 203 Abs. 1 selbständig Aufträge ausführte, nicht Gehilfe, was sich «zwar nicht schon zwingend aus dem Begriff des Gehilfen, wohl aber aus dem Grundgedanken der Vorschrift» ergebe, beispielhaft LENCKNER, in: Schönke/Schröder, 27. Aufl., D-StGB 203 N 64 m.w.H. (a.F.). Auch manifestierte sich im Gesetzgebungsprozess ein unterschiedliches Begriffsverständnis in der Schweiz und in Deutschland (insb. zur Hilfsperson, siehe vorn, III.1.2b)i). Aufgrund der engen Auslegungen von § 203 a.F. D-StGB musste die Bestimmung in der Zwischenzeit revidiert werden, um der Arbeitsteilung im Tätigkeitsbereich der Geheimnisträger besser gerecht zu werden. Die aktuell gültige Fassung ist mit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30.10.2017 (BGBl. I S. 3618) am 09.11.2017 in Kraft getreten. Ein rechtsvergleichender Blick ins österreichische Strafrecht hätte im Übrigen gezeigt, dass dort, wie in der Schweiz. ein weiter gefasstes, funktionales Verständnis der «Hilfskräfte» vorherrscht; vgl. zum Berufsgeheimnis in Österreich § 121 Ö-StGB, der allerdings nicht auf Anwälte anwendbar ist, Wiener Kommentar, LEWISCH, Ö-StGB 121 N 15, m.w.H.

Weitergabe an Schweigepflichtige den Straftatbestand erfüllen kann»[60]. Die Fussnote zu diesem Satz verweist an eine andere Stelle im Text, wo das Folgende festgehalten wird: «Auch die Weitergabe an einen anderen Amts- und Berufsgeheimnisträger kann ein Offenbaren darstellen». Hier liegt ein Fehlschluss wegen Vermischung zweier verschiedener Ausganskonstellationen vor. Wenn ein Anwalt oder eine Anwältin bspw. einer Ärztin oder einer Staatsanwältin, welche beide nach den Art. 320 und 321 StGB amtlich oder beruflich wahrgenommene Geheimnisse wahren müssen, über ein Berufsgeheimnis informiert, so ist klar, dass dies ein Offenbaren nach Art. 321 Ziff. 1 Abs. 1 StGB darstellt, wenn nicht eine gesetzliche Pflicht oder die Einwilligung des Geheimnisherrn dieses Offenbaren rechtfertigt (Konstellation 1)[61]. Trotz der Pflicht der Ärztin bzw. Staatsanwältin zur Wahrung des Amts- bzw. Berufsgeheimnisses sind sie im Verhältnis zum Anwalt unbefugte Dritte. Wie der (Haupt-)Geheimnisträger mit seinen Hilfspersonen kommunizieren darf, ist aber eine ganz andere Frage, die unabhängig von dieser Konstellation zu beantworten ist. In dieser zweiten Konstellation kann eine Weitergabe des Geheimnisses gar nie ein Offenbaren sein. Denn in einer funktionalen Betrachtung der Zusammenarbeit ist es gerade ein Definitionsmerkmal, dass die Hilfspersonen mit dem Geheimnis in Kontakt kommen bzw. dieses vom (Haupt-)Geheimnisträger erfahren, sei es, weil sie Recherchen zum Fall anstellen oder Korrespondenz dazu tippen, bearbeiten oder ar-

60 WOHLERS, 21 f. Noch deutlicher WOHLERS, 25 f. «Tatsächlich kann, …, aus der Existenz der Kategorie der Hilfspersonen als taugliche Täter *nicht* gefolgert werden, dass auch die Weitergabe an sie *für den primären Geheimnisträger* straflos sein soll. Die Kategorisierung als Hilfsperson ändert deshalb für sich gesehen nichts daran, dass die Weitergabe der Daten als Offenbarung eines Geheimnisses einzustufen ist.» (unsere Hervorhebung). Abschwächend WOHLERS, digma 2017, 114 f., wo diese Konstellation nicht mehr angesprochen wird.

61 Abweichend OGer Aargau, Urteil vom 15. Dezember 1983, SJZ 81/1985, 146 f., wonach die Weitergabe an einen aussenstehenden Berufsgeheimnisträger nicht tatbestandsmässig sei, wenn dieser auch dem Berufsgeheimnis unterstehe (unter Ärzten).

chivieren, sei es, weil sie das IT-System des (Haupt-)Geheimnisträgers regelmässig warten, mit Administratorenrechten Software-Updates im IT-System vornehmen und weitere Supportdienste leisten, wobei die geheimen Daten abrufbar bleiben (Konstellation 2). Auch den von WOHLERS aufgeführten Belegstellen lässt sich nichts zur Unterstützung seiner Position entnehmen[62]. BGE 114 IV 44, E. 3.b, BezGer Uster, Urteil vom 20. März 1996[63], BERGER[64], DONATSCH/THOMMEN/WOHLERS[65], ISENRING[66], KELLER[67], PIETH[68], RASELLI[69], STRATENWERTH/BOMMER[70] und STRATENWERTH/WOHLERS[71] beziehen sich eindeutig und ausschliesslich auf die Konstellation 1. Zudem halten auch STRATENWERTH/WOHLERS[72] explizit fest, dass eine Offenbarung gegenüber Hilfspersonen nicht tatbestandsmässig sei, was mit dem Resultat unserer Analyse übereinstimmt.

Als Ergebnis lässt sich festhalten, dass es keine Konstellation gibt, in der die Weitergabe an oder die Kenntnisnahme durch eine Hilfsperson ein Offenbaren im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB darstellt.

(ii) Zum andern vertritt WOHLERS eine äusserst restriktive Auffassung bei der Frage, wer Hilfsperson sein kann. Unsere Analyse hat gezeigt, dass im schweizerischen Strafrecht ein breit gefasstes, funktionales Verständnis der Hilfsperson gilt[73]. Demgegenüber vertritt WOHLERS

62 WOHLERS, 17 f., Fn. 65.

63 BezGer Uster, Urteil vom 20. März1996, ZR 96/1997, 266 ff. In diesem Urteil werden zudem Hilfspersonen explizit und ohne Ausnahme zum Kreis der Geheimnisträger gezählt (S. 266).

64 BERGER, recht 2000, 187.

65 DONATSCH/THOMMEN/WOHLERS, 593 m.w.H.

66 ISENRING, StGB/JStGB-Kommentar, StGB 320 N 15, StGB 321 N 10.

67 KELLER, 114 f. m.w.H.

68 PIETH, 131.

69 RASELLI, ZStR 1993, 32 f. m.w.H.

70 STRATENWERTH/BOMMER, § 61 N 7.

71 STRATENWERTH/WOHLERS, StGB 320 N 3, StGB 321 N 4.

72 STRATENWERTH/WOHLERS, StGB 320 N 3, StGB 321 N 4.

73 Siehe vorn, III.1.2b)i, mit zahlreichen Nachweisen.

eine – an deutschen Quellen zu § 203 a.F. D-StGB angelehnte – enge Auslegung. Er stützt sich dabei insb. auf eine bisher in der schweizerischen Diskussion ungebräuchliche Rechtsfigur, nämlich den «Kreis der zum Wissen Berufenen». Damit wird zum Ausdruck gebracht, dass der Geheimnisherr eine Person oder einen Kreis von Personen bestimme, mit dem oder mit denen er das Geheimnis teilen wolle[74]. Diese Rechtsfigur ist mit Blick auf die nachweislich funktionale Ausrichtung der Hilfspersonendefinition in Art. 321 Ziff. 1 Abs. 1 StGB irreführend. Der Schweizer Gesetzgeber wollte den Kreis der Personen, die das Geheimnis zur Kenntnis nehmen können, bewusst nicht auf die oder den «zum Wissen Berufenen» beschränken, sondern hat von vornherein Personen miteinbezogen, die in der Zusammenarbeit mit dem (Haupt-)Geheimnisträger mit diesen Informationen in Kontakt kommen, weil sie Dokumente schreiben, archivieren oder kopieren bzw. weil sie Dienstleistungen erbringen, die eine Kenntnisnahme von Geheimnissen mit sich bringen. Insofern ist es für Art. 321 StGB auch nicht haltbar, wenn behauptet wird, er gehe «von einem System des Informationsmanagements aus, (…) das darin besteht, dass Informationen bestimmten individuellen Geheimnisträgern anvertraut und grundsätzlich von diesem *mit niemandem* geteilt werden»[75].

v. Auswahl und Überwachung der Hilfsperson

Auch bei einer breit gefassten, funktionalen Begriffsdefinition der Hilfsperson im schweizerischen Strafrecht stellt sich die Frage, ob die Auswahl der Hilfsperson völlig dem Ermessen des Berufsgeheimnisträgers überlassen bleibt oder welche Regeln bei dieser

[74] WOHLERS, 16, 18 und 26 die entsprechenden Nachweise beziehen sich alle auf § 203 a.F. D-StGB. Ebenso WOHLERS, 20, wenn ein Outsourcingnehmer Zugriff auf die Daten und den zur Verschlüsselung verwendeten Schlüssel hat, weil er «nicht zum Kreis der zum Wissen Berufenen» gehöre. Ebenso WOHLERS, digma 2017, 116.

[75] WOHLERS, 14, Hervorhebung im Original; ebenso WOHLERS, digma 2017, 114.

Auswahl zu beachten sind[76]. Zur Beantwortung können Zivil- und Standesrecht beigezogen werden. Das Standesrecht kann zwar keine Offenbarung erlauben, die strafrechtlich verboten ist[77], aber es kann dazu beitragen, den Hilfspersonenbegriff von Art. 321 Ziff. 1 Abs. 1 StGB im Rahmen einer teleologischen Auslegung zu konkretisieren.

Die Pflicht zur Verschwiegenheit ergibt sich für Anwälte und Anwältinnen im Wesentlichen aus der Pflicht, die Persönlichkeit des Klienten nicht zu verletzen (Art. 28 ZGB), aus der schuldrechtlichen Verpflichtung zur sorgfältigen Erfüllung des Auftrags (Art. 398 Abs. 2 OR) und aus Art. 12 lit. a BGFA i.V.m. Art. 13 BGFA[78]. Der Anwalt oder die Anwältin verstösst nicht gegen seine zivil- und aufsichtsrechtlichen Sorgfaltspflichten, wenn er zur Erfüllung Hilfspersonen beizieht[79]. Gemäss der Botschaft des Bundesrates vom 28. April 1999 über das BGFA entspricht der Begriff der Hilfskraft im Sinn von Art. 13 Abs. 2 BGFA demjenigen der Hilfsperson in Artikel 101 OR[80]. Hilfspersonen sind damit Dritte, die vom Anwalt oder der Anwältin mit bestimmten Aufgaben betraut werden[81].

Wenn der Anwalt oder die Anwältin eine Hilfsperson beizieht, profitiert er oder sie nicht nur von den Vorteilen der Arbeitsteilung, sondern haftet auch für allfällige Nachteile, die sich dem Klienten daraus ergeben können[82]. So haften sie nach Art. 101 OR für alle in Erfüllung

---

76 WOHLERS, 16; WOHLERS, digma 2017, 115, ist aufgrund seines engen Auslegungsansatzes der Ansicht, dass die Kontrolle über den Kreis der Geheimnisberechtigten nicht dem Anwalt bzw. der Anwältin überantwortet werden könne.

77 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 16; siehe auch BSK-OR I, WEBER, OR 398 N 11.

78 Eingehend: CR-LLCA, MAURER/GROSS, LLCA 13 N 11 ff.; SCHILLER, Rn. 383 ff.

79 BSK-OR I, WEBER, OR 398 N 3; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 50.

80 BBl 1999 6013, 6056.

81 BOHNET/MARTENET, § 11 N 1861; CHAPPUIS, 178 ff; FELLMANN, Rn. 555 und 634; CR-LLCA, MAURER/GROSS, LLCA 13 N 93; NATER/ZINDEL in: Fellmann/Zindel, BGFA 13 N 51.

82 BGE 114 Ib 67, E. 2.c; BSK-OR I, WIEGAND, OR 101 N 2.

der Schuldpflicht durch die Hilfsperson verursachten Schäden, sofern ihnen diese hypothetisch vorwerfbar wären. Ob eine vertragliche Freizeichnung mit Art. 101 Abs. 3 OR und dem BGFA vereinbar ist, ist umstritten[83], hier aber nicht entscheidend. Denn Art. 13 Abs. 2 BGFA verlangt von Anwältinnen und Anwälten, dass sie durch Auswahl, Überwachung und Instruktion der Hilfspersonen für die Wahrung des Berufsgeheimnisses sorgen[84]. Unternimmt ein Anwalt oder eine Anwältin nicht alles Zumutbare damit die Hilfsperson das Berufsgeheimnis wahrt, verstösst er oder sie gegen diese Berufsregel[85]. Die Lehre fordert, dass Hilfspersonen vertraglich zur Geheimhaltung verpflichtet werden[86], betont aber, dass je nach Grösse und Tätigkeit der Kanzlei ein eigentliches Sicherheitsdispositiv erforderlich sein kann[87]. Eine sorgfältige Berufsausübung erfordert folglich, dass Informationen nach dem «*Need-to-Know*»-Grundsatz geteilt werden[88]. Es kann sich deshalb aufdrängen, bei besonders sensiblen Informationen den Kreis der einbezogenen Hilfspersonen enger zu fassen[89].

---

83 Siehe REHMANN, SJZ 2017, 134; SCHILLER, Rn. 1627 ff.; FELLMANN, in: Fellmann/Zindel, BGFA 12 N 27a.

84 SCHILLER, Rn. 540 ff.; siehe auch CHAPPUIS/ALBERINI, AwR 2017, 341.

85 SCHILLER, Rn. 540; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56 f.

86 CR-LLCA, MAURER/GROSS, LLCA 13 N 101; SCHILLER, Rn. 541; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56; siehe auch DSB ZÜRICH, Tätigkeitsbericht 2017, 18.

87 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56 f. Zu denken wäre z.B. an das Schlüsselmanagement, das bei IaaS-Service Modellen in der Verantwortung der Kanzlei bleibt (siehe II.3.2) oder die Zugangskontrolle bei IaaS und SaaS Service-Modellen (II.3.3), die immer in der Verantwortung der Kanzlei bleibt (siehe auch IV.3.1d)).

88 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 43.

89 So werden z.T. bei Übernahmen börsenkotierter Unternehmen oder Mandaten von Personen des öffentlichen Interesses sog. Chinese Walls eingerichtet, siehe zur Gestaltung eines Data Rooms im Rahmen einer Due Dilligence: ROSENTHAL, in: Rosenthal/Jöhri, OR 328b N 57. Z.T. wird den Hilfspersonen, die zur Rechtsrecherche beigezogen werden, die Identität des Mandanten nicht bekanntgegeben. Bei Banken ist die Errichtung von Chinese Walls im Rahmen einer Übernah-

Damit erscheint klar, dass der Geheimnisträger nicht völlig frei ist, wen er als Hilfsperson hinzuzieht. Der Gesetzgeber anerkannte aber die Notwendigkeit der Mitwirkung von Hilfspersonen und überliess die Konkretisierung des Kreises von Hilfspersonen der Auslegung. Eine jeweils explizite Bestimmung der Hilfsperson durch den Geheimnisherrn wurde beim Erlass der Norm nicht diskutiert und wird vom Gesetz auch nicht verlangt[90]. Innerhalb des gesetzlichen Rahmens muss die Lösung deshalb nach dem Sinn und Zweck der Norm herausgearbeitet werden. Das Leitprinzip kann dabei wie folgt formuliert werden: Alle Tätigkeiten, die objektiv bei einer sinnvollen Arbeitsteilung innerhalb einer Arztpraxis, Anwaltskanzlei oder sonstigen Tätigkeit eines Berufsgeheimnisträgers notwendig und im beruflichen Kontext bei der Bewältigung der administrativen Prozesse üblich sind, können vom (Haupt-)Geheimnisträger auf Hilfspersonen übertragen werden und zwar ohne spezifische Einwilligung des Geheimnisherrn[91]. Bei der Auswahl der Hilfsperson sind die zivil- und

me sogar eine aufsichtsrechtliche Marktverhaltensregel (siehe TSCHÄNI/DIEM, 129, insb. Fn. 351).

90 So ist es bis heute völlig unüblich, für den Beizug von Sekretariatspersonal innerhalb einer Anwaltskanzlei eine Einwilligung einzuholen.

91 A.M. WOHLERS, 19, unter Bezugnahme auf den «Kreis der zum Wissen Berufenen», wobei die zur Unterstützung dieser Position zitierte ALTHAUS STÄMPFLI, 143 (zu Art. 47 BankG), eher der hier vertretenen Position entspricht: «Grundsätzlich ist davon auszugehen, dass der durchschnittliche Kunde darauf vertraut, dass die Informationen und Daten, welche er seinem Kundenbetreuer anvertraut, nur denjenigen Personen weitergegeben werden, welche einen *Beitrag an die vom Kunden beanspruchten Dienstleistungen leisten*. Dies steht nicht im Widerspruch zum Interesse des Kunden und damit zum Grundsatz 'Kenntnis nur soweit nötig.» Auch bei einem Mandanten eines Anwalts bzw. einer Anwältin oder einem Patienten eines Arztes bzw. einer Ärtzin ist davon auszugehen, dass diese Geheimnisherren mit der nützlichen und üblichen Arbeitsteilung in der Kanzlei bzw. der Praxis rechnen. ALTHAUS STÄMPFLI, 143 (zu Art. 47 BankG): «Jeder Kunde weiss, dass eine Bank oder ein Finanzintermediär heute als arbeitsteilige Organisation ihre Dienstleistungen durch verschiedene Abteilungen erbringt.» Immerhin soll nach WOHLERS, 21, ein (mutmassliches) Einverständnis dann angenommen werden dürfen, «wo die Offenbarung zur sachgerechten Erledigung der

standesrechtlichen Pflichten zu beachten, die bei der teleologischen Auslegung ergänzend Berücksichtigung finden und zu einer sinnvollen Eingrenzung führen. Das Geheimnis wird durch den Beizug von Hilfspersonen keineswegs schutzlos, weil die Hilfspersonen, wie erwähnt[92], mit der gleichen Strafandrohung zur Geheimhaltung verpflichtet sind.

Ist der Anwalt oder die Anwältin allgemein nicht frei in der Entscheidung, mit wem er geheime Informationen teilt, so gilt dies auch für die Wahl des Cloud-Providers als Hilfsperson[93]. Wie bei anderen Hilfspersonen, muss der Anwalt oder die Anwältin auch den Cloud-Provider vertraglich zur Einhaltung des Berufsgeheimnisses verpflichten. In der Praxis wird er oder sie die AGB der Cloud-Provider entsprechend zu prüfen haben. Aus dem BGFA ergibt sich ferner, dass der Anwalt oder die Anwältin die Einhaltung dieser Verschwiegenheitsverpflichtung in zumutbarer Weise zu überwachen hat.

Teilweise wird gefordert, Anwälte und Anwältinnen hätten für eine Speicherung der Daten in der Schweiz zu sorgen bzw. einen Schweizer Anbieter zu wählen, weil ansonsten ausländische Behörden, die nicht an das Berufsgeheimnis gebunden seien, auf die Daten zugreifen könnten[94]. Zunächst kann es hierbei nur auf den Sitz des Cloud-Providers oder den tatsächlichen Arbeitsort der Techniker ankommen, denn am blossen Serverstandort fehlt ein Rechtssubjekt, gegen das solche Verfügungen vollstreckt werden könnten. Dogmatisch lässt sich aber auch diese Unterscheidung nicht rechtfertigen, denn der Beizug von ausländischen Hilfspersonen ist unter Art. 321 StGB

vom Geheimnisherrn gewünschten Dienstleistung unabdingbar» sei, mit Verweis auf KELLER, 108.

92 Siehe dazu vorn, III.1.2b)i.

93 WOHLERS, digma 2017, 115, scheint hingegen davon auszugehen, dass die Auswahl der Hilfsperson dem Gutdünken des Anwalts bzw. der Anwältin überlassen sei.

94 CHAPUIS/ALBERINI, AwR 2017, 341; ähnlich: SCHWANINGER/LATTMANN, Jusletter 11. März 2013, Rn. 31.

grundsätzlich erlaubt und bei Kommunikationsvorgängen ist es oft nicht vermeidbar, auf ausländische Hilfspersonen zuzugreifen. Eine Anwaltskanzlei, die mit ausländischen Gegenparteien, Gerichten, Zeugen oder Gutachtern kommuniziert, kommt nicht umhin, dem Berufsgeheimnis unterstehende Informationen in die Hände ausländischer E-Mail-Provider, Poststellen oder Telekommunikationsanbieter zu geben. Der Anwalt oder die Anwältin muss unter den für das Berufsgeheimnis relevanten Gesichtspunkten je nach Sensibilität der Informationen entscheiden, ob der Beizug der fraglichen ausländischen Hilfsperson risikoadäquat ist. Eine allgemeine Pflicht nur Schweizer Cloud-Provider zu wählen, besteht aufgrund von Art. 321 StGB nicht[95]. Bei der Beurteilung der Risikoadäquanz ist vor allem die Sensitivität der Daten, aber auch die zu erwartende Vertrags- und Gesetzestreue des ausländischen Cloud-Providers sowie die tatsächliche Wahrscheinlichkeit eines Zugriffs auf die Daten zu berücksichtigen. Diese Risikoeinschätzung kann je nach Tätigkeit von Anwältinnen und Anwälten unterschiedlich ausfallen; besondere Vorsicht dürfte etwa bei der Beratung ausländischer Klienten in Steuerfragen und bei politisch exponierten Mandanten angezeigt sein[96].

vi. Zwischenfazit

Zum Begriff der Hilfsperson kann festgehalten werden, dass die hier vertretene, breit gefasste, funktionale Auslegung durch den Wortsinn

---

[95] Je nach Tätigkeit der Kanzlei könnte sich eine solche Pflicht aus dem Verbot des wirtschaftlichen Nachrichtendienstes nach Art. 273 StGB ergeben, gemäss dem niemand einem ausländischen Destinatär ein Schweizerisches Geschäfts- und Fabrikationsgeheimnis zugänglich machen darf (in diese Richtung: WAGNER/ZWIRNER, 174 Fn. 42; zurückhaltend: VLCEK, 176). Diese Bestimmung ist aber restriktiv auszulegen (ROSENTHAL, in: Rosenthal/Jhöri, StGB 273 N 64), bzw. es wird angemahnt, dass der Bundesrat die notwendige Ermächtigung zur Strafverfolgung (Art. 66 StBOG) bei im Ausland begangenen Taten nur zurückhaltend erteilen könne (BSK-Strafrecht II, HUSMANN, StGB 273 N 79).

[96] Siehe dazu auch die datenschutzrechtliche Analyse der Auslagerung einer Datenbearbeitung in die USA, IV.3.1f).

von Art. 321 StGB, den systematischen Kontext, die historischen Rechtsetzungsquellen und die teleologischen Überlegungen gestützt wird. Diese Auslegung wird denn auch von der h.L. vertreten[97]. Die vor allem am alten deutschen Recht orientierte, enge Auffassung von WOHLERS kann nicht überzeugen.

In der Anwendung auf die arbeitsteilige Tätigkeit in Anwaltskanzleien gilt damit als gesichert, dass alle Personen, die bei der Berufstätigkeit des (Haupt-)Geheimnisträgers in einer Weise unterstützend mitwirken und dadurch von den Geheimnissen Kenntnis erhalten können, als Hilfspersonen anzusehen sind. Es bedarf dazu keiner expliziten Einwilligung durch den Geheimnisherrn. Zu den Hilfspersonen zählen IT-Verantwortliche innerhalb der Anwaltskanzlei ebenso wie externe IT-Dienstleistungsunternehmen, welche die Informationsverarbeitung, -speicherung und -archivierung der Anwaltskanzlei sicherstellen, das Betriebssystem warten und Sicherheitsmassnahmen treffen. Die Hilfspersonen müssen nicht in einem Arbeitsverhältnis mit dem (Haupt-)Geheimnisträger stehen und sie können ihre Hilfstätigkeit auch ausserhalb der Büroräumlichkeiten des (Haupt-)Geheimnisträger erbringen. Auch Hilfstätigkeiten im Ausland sind nicht ausgeschlossen. Anbieter von Cloud-Lösungen (IaaS, SaaS) gehören damit ebenfalls zum Kreis der Hilfspersonen.

Der Geheimnisschutz wird durch den Einbezug von Hilfspersonen im Allgemeinen und durch das Nutzen der Dienste von Cloud-Providern im Speziellen keineswegs obsolet[98], weil die Geheimhaltungspflichten und Strafdrohungen auch für alle Hilfspersonen gelten. Ausserdem setzt das Datenschutzrecht der externen Auftragsdatenverarbeitung Grenzen und der (Haupt-)Geheimnisträger wird durch die Hilfspersonenhaftung nach Art. 101 OR in die Pflicht genommen.

---

97 Siehe vorn, III.1.2b)i.

98 So aber WOHLERS, 10.

c) Tathandlung: Offenbaren

Das objektive Tatbestandsmerkmal des Offenbarens ist erfüllt, wenn der Geheimnisträger das Geheimnis einer dazu nicht ermächtigten Drittperson[99] zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht. Dies kann auf beliebige Art und Weise geschehen. Die folgenden Tathandlungsvarianten stehen im Vordergrund[100]: die mündliche oder schriftliche Mitteilung, das Aushändigen von Schriftstücken oder anderen Sachen, die das Geheimnis verraten, der Versand von elektronischen Daten (Text, Bild, Ton, Video) sowie das Zugänglichmachen von elektronischen Daten auf einem für mindestens einen unbefugten Dritten zugänglichen Speichermedium. Die Tat kann aber auch durch unechte Unterlassung begangen werden[101], z.B. durch eine unzureichende Aufbewahrung von Akten[102].

Auf die dogmatische Unschärfe, dass zur Vollendung nach h.L. die Kenntnisnahme durch mindestens einen unbefugten Dritten vorausgesetzt wird, was bei einem schlichten Zugänglichmachen oder Liegenlassen der Akten im Büro noch nicht erfüllt sein kann, wurde vorn

---

99 PK-StGB, TRECHSEL/VEST, StGB 321 N 23 «(mindestens) ein Aussenstehender»; Hilfspersonen sind ermächtigte Personen. Ihnen gegenüber kann das Geheimnis nicht in tatbestandsmässiger Art offenbart werden (siehe vorn, III.1.2b)ii), a.M. WOHLERS, 26.

100 BGE 75 IV 71, E. 1; 112 Ib 606, E. b; DONATSCH/THOMMEN/WOHLERS, 593 m.w.H.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; STRATENWERTH/BOMMER, § 61 N 19; WOHLERS, 17; WOHLERS, digma 2017, 115; vgl. FELLMANN, Rn. 560.

101 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; PK-StGB, STRATENWERTH/BOMMER, § 61 N 7 und 19; STRAUB, AJP 2010, 552 und 555; TRECHSEL/VEST, StGB 321 N 23.

102 Betreffend die Anforderungen für die Archivierung der Akten können die datenschutzrechtlichen Vorgaben aus Art. 7 DSG sowie Art. 8 VDSG herangezogen werden, da es sich bei den Akten regelmässig um Datensammlungen im Sinn des DSG handelt, welche oft besonders schützenswerte Daten i.S. v. Art. 3 lit. c DSG umfassen. Anwälte sind von der Meldepflicht gemäss Art. 11a DSG befreit, vgl. BSK-DSG/BGÖ, BLECHTA, DSG 11a N 14d. Zur Aufbewahrung: BSK-DSG/BGÖ, BLECHTA, DSG 7 N 7 ff.

schon hingewiesen[103]. Sogar wenn der Empfänger die geheimzuhaltende Tatsache bereits gerüchteweise kennt oder vermutet, kann ein Geheimnis offenbart werden, wenn dadurch verlässliches und sicheres Wissen entsteht[104].

Bei anonymisierten oder verschlüsselten Informationen bzw. Daten, deren Inhalt nicht eruiert werden kann, liegt kein Offenbaren vor, selbst wenn Aussenstehende die Daten an sich zur Kenntnis nehmen können[105]. Die Archivierung verschlüsselter Daten in der Cloud (IaaS) erfüllt daher schon den objektiven Tatbestand von Art. 321 StGB nicht. Bei SaaS-Modellen (siehe Szenario 2, II.3.3) verfügt der Cloud-Provider technisch gesehen über Zugang zu den im Dokument gespeicherten Daten. In diesen Konstellationen ist ein Offenbaren möglich.

Nach der vorn dargelegten Auslegung sind Personen, die für die IT-Dienste des Anwalts oder der Anwältin zuständig sind oder Cloud-Lösungen für ihn betreiben – auch wenn sie externe Anbieter sind –, Hilfspersonen im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB. Ihnen gegenüber dürfen die Informationen der Mandanten zugänglich gemacht werden, ohne dass es sich dabei um ein Offenbaren handelt[106]. Mit anderen Worten: Die Tatbestandsmässigkeit entfällt bei der Weitergabe oder Zugänglichmachung von Daten zwischen (Haupt-)Geheimnisträger und Hilfspersonen.

---

103 Siehe vorn, III.1.1.

104 BGE 75 IV 71, E. 1; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19.

105 BERGER, recht 2000, 191 m.w.H.; BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 13; PK-StGB, TRECHSEL/VEST, StGB 321 N 23; WOHLERS, 20; EDÖB, 14. Tätigkeitsbericht, 51.

106 A.M. WOHLERS, 20, der Outsourcingnehmer nicht als Hilfspersonen betrachtet. Sobald sie die geheimen Informationen des Geheimnisherrn entschlüsseln können, geht er von einem Offenbaren aus. Ebenso bezüglich Wartung von Software.

1.3 Subjektiver Tatbestand

Subjektiv ist Handeln mit Vorsatz erforderlich, wobei Eventualvorsatz genügt. Wenn der Täter also mit der Möglichkeit rechnet, ein Geheimnis zu offenbaren, und diese Möglichkeit in Kauf nimmt, erfüllt er dieses Tatbestandsmerkmal (Art. 12 Abs. 2 StGB)[107].

Relevanz hat der subjektive Tatbestand, falls eine Hilfsperson ein Geheimnis einem unbefugten Dritten offenbart. Es stellt sich dann die Frage, ob auch der (Haupt-)Geheimnisträger wegen Berufsgeheimnisverletzung strafbar sein kann. Dies wäre zu bejahen, wenn dem (Haupt-)Geheimnisträger von vorherein bekannt ist oder es ihm zumindest möglich erscheint, dass es zu einer Offenbarung durch die Hilfsperson kommen wird, und er diesen Erfolg in Kauf nimmt. In der Regel wird dies aber gerade nicht der Fall sein, so dass nur die Hilfsperson strafrechtlich zur Rechenschaft gezogen wird. Der (Haupt-)Geheimnisträger kann aber allenfalls nach Art. 101 OR zivilrechtlich belangt werden.

1.4 Rechtswidrigkeit

Gemäss Art. 321 Ziff. 2 StGB entfällt die Strafbarkeit, wenn der Täter das Geheimnis aufgrund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat. Gemäss Ziff. 3 bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde vorbehalten.

Unsere Analyse hat gezeigt, dass IT-Verantwortliche innerhalb der Anwaltskanzlei und externe Anbieter von Cloud-Lösungen als Hilfspersonen im Sinn von Art. 321 Ziff. 1 Abs. 1 StGB anzusehen sind. Diese Hilfspersonen können ihre Tätigkeit für den Geheimnisträger

[107] PK-StGB, TRECHSEL/VEST, StGB 321 N 26; STRATENWERTH/BOMMER, § 61 N 20; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 21.

auch ohne Einwilligung des Geheimnisherrn ausüben[108]. In diesem Abschnitt werden daher die Voraussetzungen und Wirkungen einer Einwilligung des Geheimnisherrn im Kontext der Auslagerung von IT-Dienstleistungen in eine Cloud nur mit Blick auf eine zusätzliche (rechtfertigende) Absicherung behandelt[109]. Im Sinn einer solchen zusätzlichen Absicherung kann es sich empfehlen, vom Geheimnisherrn im Rahmen des Mandatsvertrages vorgängig eine Einwilligung für den Einbezug eines Anbieters von Cloud-Diensten, aber auch generell für regelmässig eingesetzte Hilfspersonen (z.B. Substituten, IT-Verantwortliche) einzuholen. Dies schafft klare Verhältnisse gegenüber den Klienten und wirkt im Straf- und Datenschutzrecht[110] rechtfertigend[111].

Sofern ein Einverständnis in die gänzliche Preisgabe des Geheimnisses vorliegt, ist das Verhalten nicht mehr tatbestandsmässig, weil kein Unrecht i.S. einer Verletzung der Privatsphäre des Geheimnisherrn mehr entstehen kann. Wird jedoch die Preisgabe nur an gewisse Personen oder Stellen gestattet, hat die Einwilligung den Charakter eines Rechtfertigungsgrunds[112]. Bei der Anwaltstätigkeit geht es in der Re-

---

108 Siehe vorn, III.1.2b).

109 Für BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 10, dient die Einwilligung dazu, sich «nicht dem Risiko eines negativen richterlichen Urteils auszusetzen». Weitere Rechtfertigungsgründe kommen nur in seltenen Ausnahmefällen zur Anwendung, siehe WOHLERS, 26 f.

110 Siehe dazu hinten, IV.

111 Dazu hinten, IV.3.1b) und IV.3.2a); WOHLERS, 26, kommt aufgrund seiner engeren Auslegung zum Schluss, dass die Auslagerung von Hilfstätigkeiten an externe Dritte nur dann straflos sein könne, wenn ein Rechtfertigungsgrund, insb. eine Einwilligung, vorliege.

112 OGer Zürich, Urteil vom 30. August 2016, SB160142, E. 3.4.1.b; DONATSCH/THOMMEN/WOHLERS, 599; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

gel um letztere Konstellation. Es gelten die allgemeinen Grundsätze der rechtfertigenden Einwilligung[113].

a) Einwilligung durch den Rechtsgutsträger

Vorausgesetzt ist die Dispositionsbefugnis über das Rechtsgut, d.h. es muss sich um ein Individualrechtsgut handeln. Diese Voraussetzung ist erfüllt[114]. Der Geheimnisherr kann die Einwilligung nach Person, Gegenstand, Adressat und Zeitpunkt der Bekanntgabe beschränken[115].

b) Einwilligungsfähigkeit

Für eine rechtswirksame Einwilligung wird Urteilsfähigkeit verlangt. Zum Zeitpunkt der Einwilligung muss der Geheimnisherr die tatsächlichen Umstände richtig erfassen und entsprechend dieser Wahrnehmung sein Verhalten steuern können. Die Urteilsfähigkeit ist vom Gesetz negativ umschrieben, wobei in der Regel von der Urteilsfähigkeit auszugehen ist (vgl. Art. 16 ZGB)[116]. Da die Urteilsfähigkeit relativ ist, also je nach sozialem Kontext und Komplexität des zu beurteilenden Sachverhalts gegeben sein oder fehlen kann, können auch handlungsunfähige Personen unter Umständen als urteilsfähig gelten. Fehlt die Urteilsfähigkeit, obliegt die Entscheidung ihren gesetzlichen

---

113 Allgemein zur Einwilligung: SEELMANN/GETH, 50; PK-StGB, TRECHSEL/GETH, StGB 14 N 11 m.w.H.

114 Art. 321 Ziff. 2 StGB, siehe vorn, III.1.1. Die Person des Berechtigten ist identisch mit dem zur Antragstellung legitimierten Verletzten, BGE 75 IV 75 E. 3; PK-StGB, TRECHSEL/VEST, StGB 321 N 28. Es kann nur der Geheimnisherr selbst seine Einwilligung geben, wobei die Person, welche das Geheimnis betrifft, nicht mit der Person, die das Geheimnis anvertraut hat, identisch sein muss, BLASS, SJZ 1966, 337; CR-CP II, CHAPPUIS, CP 321 N 140; DUPUIS ET AL., CP 321 N 38, 40; KELLER, 137; REHBERG, Schweizerische Ärztezeitung 1969, 235; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

115 DE HALLER, Schweizerische Versicherungs-Zeitschrift, 1980, 9; DUPUIS ET AL., CP 321 N 42; KELLER, 146; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

116 BSK-ZGB I, BIGLER-EGGENBERGER/FANKHAUSER, ZGB 16 N 2 m.w.H.

Vertretern, selbstredend innerhalb der Grenzen der Obhutspflicht[117]. Bei urteilsunfähigen Patienten wird das Geheimhaltungsinteresse vermutet[118].

c) Freiheit von Willensmängeln und «*informed consent*»

Die Zustimmung des Geheimnisherrn muss aus freiem Willen erfolgen. Dabei muss der Geheimnisherr seine Einwilligung in voller Kenntnis von Art und Tragweite der Geheimnisoffenbarung und aller wesentlichen Umstände äussern. Ferner darf keine Beeinträchtigung der Willensbildung durch Zwang, Drohung oder Täuschung vorliegen[119].

Damit dies möglich ist, muss der Geheimnisherr über den Umgang mit den Akten, Daten und Informationen hinreichend informiert werden («*informed consent*»)[120]. Folglich muss der Geheimnisherr über Gegenstand, Zweck und Umfang der beabsichtigten Datenweitergabe aufgeklärt werden. Dies kann im Rahmen einer Vollmacht oder eines Mandatsvertrags spezifiziert werden.

WOHLERS argumentiert, dass eine Einwilligungserklärung zwar grundsätzlich auch formularmässig erfolgen kann, so bspw. bei der Aufnahme einer Kundenbeziehung durch eine Unterschrift auf einem Anmeldeformular mit entsprechendem Hinweis. Hingegen erfülle das Einholen einer umfassenden, unspezifizierten Einwilligung durch

---

117 Eine Stellvertretung bei Entscheidungen im Intimbereich ist z.B. nicht möglich. BSK-ZGB I, BIGLER-EGGENBERGER/FANKHAUSER, ZGB 16 N 5 ; CR-CP II, CHAPPUIS CP 321 N 141 ; CORBOZ, SJ 1993, 91 ff.; DONATSCH/THOMMEN/WOHLERS, 599; DUPUIS ET AL., CP 21 N 40; KELLER, 140; SEELMANN/GETH, 52; STRATENWERTH, § 10 N 21; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

118 PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

119 BOHNET/MARTENET, § 11 N 1905; KELLER, 141 ff.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; SEELMANN/GETH, 53; STRATENWERTH, § 10 N 22; WOHLERS, 29; WOLFFERS, 39.

120 OGer Zürich, Urteil vom 30. August 2016, SB160142, E. 3.4.1.b, am Beispiel der Weitergabe von Patientendaten an Dritte; KELLER,142; PIETH, 131.

Formulare und/oder Allgemeine Geschäftsbedingungen die Voraussetzung einer wirksamen Einwilligung nicht[121]. Fraglich ist somit, ob eine Einwilligung zum Anfangszeitpunkt eines Mandatsverhältnisses mit Blick auf die Bestimmtheit des zu offenbarenden Geheimnisses möglich ist. WOHLERS zieht dabei den Vergleich zum Patienten, der gegenüber der Krankenkasse eine generelle Entbindung des Arztes von der Schweigepflicht unterzeichnet, wobei sich der Patient zu diesem Zeitpunkt der Tragweite seiner Erklärung noch nicht bewusst sein könne. Dieser Vergleich schlägt jedoch insofern fehl, als beim Mandatsverhältnis zu einem Anwalt oder einer Anwältin die relevanten Geheimnisse bereits hinreichend bestimmbar sind und sich der Klient aufgrund der Aufklärung über den Umgang mit den Daten sehr wohl «informiert» entscheiden kann[122].

d) Form und Zeitpunkt der Einwilligung

Die Einwilligung muss nach den allgemeinen Grundsätzen vor der Ausführung der Tathandlung erfolgen[123]. Nicht haltbar ist die Ansicht, eine Einwilligung könne auch nach der Offenbarung des Geheimnisses rechtfertigend wirken[124]. Nach Vollendung der Tat bleibt dem Geheimnisherrn «nur» die Möglichkeit, auf den Strafantrag zu verzichten (oder diesen zurückzuziehen). Soweit Anwaltskanzleien die Dienste von Cloud-Providern bereits in Anspruch nehmen, erscheint es für laufende Mandatsverhältnisse immerhin denkbar, von den Klienten nachträglich die Zustimmung zur Nutzung dieser Dienste einzuholen. Diese Zustimmung ist für die künftige Nutzung als Einwilligung zu verstehen. Für die bereits erfolgte Nutzung kommt die Einwilligung einer Desinteressement-Erklärung oder, falls

121 WOHLERS, 28.

122 BERGER, recht 2000, 193; SCHÄFER, 55; STOCKER, 249.

123 BOHNET/MARTENET, § 11 N 1908; CORBOZ, SJ 1993, 93; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; SEELMANN/GETH, 50.

124 CR-CP II, CHAPPUIS, CP 321 N 146; CORBOZ, SJ 1993, 93; DUPUIS ET AL., CP 321 N 44.

die Formvorschriften eingehalten sind (Art. 302 Abs. 2 StPO), einem Verzicht gemäss Art. 30 Abs. 5 StGB gleich[125].

Die Einwilligung des Berechtigten bedarf von Gesetzes wegen keiner besonderen Form[126], wobei die einseitige Willenserklärung entweder ausdrücklich oder konkludent zum Ausdruck gebracht werden kann[127].

Bei der konkludenten Zustimmung soll der Wille des Geheimnisherrn, auf die Wahrung des Geheimnisses verzichten zu wollen, klar zum Ausdruck kommen, wobei es gemäss Bundesgericht für die Befreiung vom Berufsgeheimnis bspw. genügt, wenn der Berechtigte den Geheimnisträger als Zeugen im Prozess anruft[128]. Im medizinischen Bereich wird davon ausgegangen, dass die Einwilligung auch für den notwendigen Beizug von Spezialärzten gilt, sofern sich aus einem Behandlungsauftrag nichts anderes ergibt. Auch im Verhältnis zwischen einweisendem und behandelndem Arzt sowie bei der Weiter- und Nachbehandlung liegt der gegenseitige Informationsaustausch im Interesse des Patienten[129].

Gemäss DONATSCH/THOMMEN/WOHLERS rechtfertigt allein die Tatsache, dass die Weitergabe von Informationen im Interesse des Patienten oder Klienten liegen kann, die Annahme einer konkludenten Einwilligung nicht. Vielmehr muss der Wille auf die Wahrung des

125 BSK-Strafrecht I, RIEDO, StGB 30 N 119 ff. m.w.H. Die Verzichtserklärung kann auch gegenüber Dritten insbes. dem Täter ausgesprochen werden.

126 Eine ausdrückliche, schriftliche Einwilligung ist jedoch zu empfehlen.

127 BGE 97 II 369, 370; 98 IV 217, E. 2; BezGer Uster, ZR 96/1997, 295; CR-CP II, CHAPPUIS CP 321 N 144; DE HALLER, Schweizerische Versicherungs-Zeitschrift 1980, 19; DONATSCH/THOMMEN/WOHLERS, 599; DUPUIS ET AL., CP 321 N 41; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28; UTTINGER/LIEBRENZ, Schweizerische Ärztezeitung 2014, 1745.

128 BGE 97 II 369, 370; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22.

129 KELLER, 114 ff; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

Geheimnisses verzichten zu wollen, klar zum Ausdruck kommen[130]. Gemäss KELLER muss nach den Erfahrungen des Lebens aufgrund der konkludenten Handlung auf eine Einwilligung geschlossen werden können[131]. Von einer stillschweigenden Einwilligung des Patienten zur Offenbarung der Tatsachen an die übrigen Ärzte eines Ärztekollegiums kann bspw. ausgegangen werden, wenn diese den Patienten gemeinsam behandeln. So muss bei gemeinsamer ärztlicher Betreuung nicht jeder Arzt selbst neu die Krankengeschichte aufnehmen und alle Untersuchungen selbst durchführen[132]. Ebendies wird man auch für die Bearbeitung eines Mandates durch mehrere Anwältinnen und Anwälte und für den Beizug eines Cloud-Providers annehmen können.

Wird der Klient durch einen Anwalt oder eine Anwältin zur zusätzlichen Absicherung um eine Einwilligung in die Bekanntgabe von Geheimnissen ersucht, so kann der Klient diese formlos erteilen. Von einer konkludenten Einwilligung wird man allerdings nur ausgehen können, wenn der Klient eine Handlung vornimmt, die sein eindeutiges Einverständnis mit der Offenbarung geheimer Informationen an den Cloud-Dienstleister zu erkennen gibt. Dies ist bereits der Fall, wenn die Anwältin oder der Anwalt den Klienten auf die Nutzung eines Cloud-Providers für das Speichern und Bearbeiten der das Mandat betreffenden Daten aufmerksam macht und der Klient das Mandatsverhältnis ohne weiteres fortführt. Noch deutlicher wäre eine explizite Einwilligung.

e) Handeln in Kenntnis der Einwilligung

Eine Einwilligung kann nach den allgemeinen Regeln nur dann rechtfertigend wirken, wenn der «Täter» von der Einwilligung vor seinem

130 DONATSCH/THOMMEN/WOHLERS, 599; BezGer Uster, ZR 96/1997, 289-303.

131 KELLER, 144.

132 KELLER, 115; REHBERG, Schweizerische Ärztezeitung 1969, 235; SCHÄFER, 29; TIMM, 33.

Handeln Kenntnis genommen hat[133]. Handelt er ohne dieses Wissen, befindet er sich in einem Irrtum, der sich zu seinen Ungunsten auswirkt, sein Verhalten würde also als Versuch der Tatbegehung angesehen.

Wird eine Einwilligung im Rahmen einer Vollmacht oder eines Mandatsvertrags ausgesprochen, worin die Modalitäten des Umgangs mit den Akten, Daten und Informationen des Klienten umfassend festgehalten werden, stellt dieses Kriterium vorliegend kein Problem dar.

f) Widerrufbarkeit der Einwilligung

Als Ausfluss der allgemeinen Handlungsfreiheit ist die Einwilligung als einseitige, empfangsbedürftige, rechtsgestaltende Willenserklärung jederzeit frei widerruflich. Der Widerruf kann aber nur für die Zukunft Wirkung entfalten[134].

1.5 Strafantrag

Eine Strafverfolgung ist vom Strafantrag des Geheimnisherrn abhängig. Zum Stellen eines Strafantrags nach Art. 321 StGB berechtigt ist nicht nur der Klient, sondern jeder Geheimnisherr, d.h. jede direkt von der Offenbarung des Geheimnisses betroffene Person, die nicht Klient des Anwalts oder der Anwältin zu sein braucht[135].

---

133 KELLER, 139; SEELMANN/GETH, 53; STRATENWERTH, § 10 N 24.

134 CR-CP II, CHAPPUIS, CP 321 N 146; KELLER, 143 f.; SEELMANN/GETH, 50; SIEBEN, 88.

135 NIGGLI, AwR 2006, 279; RIEDO, 217 f.; PK-StGB, TRECHSEL/VEST, StGB 321 N 27.

1.6 Internationale Sachverhalte

a) Strafanwendungsrecht und Tatbestandsmässigkeit

Das Strafanwendungsrecht legt fest, wann eine Norm des Schweizer Strafrechts in räumlicher Hinsicht Geltung beanspruchen kann[136]. Ob es sich bei der Frage der Anwendung des Schweizer Strafrechts um eine Prozessvoraussetzung, Zurechnungsregel *sui generis* oder eine objektive Bedingung der Strafbarkeit handelt, ist umstritten[137]. Einigkeit besteht aber darüber, dass die Frage der Geltung des Schweizer Strafrechts der strafrechtlichen Zurechnung im engeren Sinne vorausgeht[138]. Die Frage, ob ein Verhalten der Schweizer Strafhoheit untersteht, muss damit unabhängig und vor der Frage untersucht werden, ob dieses Verhalten auch einen Tatbestand des Schweizer Strafrechts erfüllt.

b) Strafanwendung bei Verletzungs- und Erfolgsdelikten

Da Art. 321 StGB als Verletzungs- und Erfolgsdelikt ausgestaltet ist[139], stehen nach Art. 3 Abs. 1 i.V.m. Art. 8 StGB (Territorialitäts- und beschränktes Ubiquitätsprinzip) zwei Anknüpfungspunkte für die schweizerische Strafhoheit im Vordergrund: der Handlungsort und der Erfolgsort[140]. Das wichtigste Anknüpfungselement im Strafan-

---

136 SCHWARZENEGGER, ZStrR 2000, 114; GLESS, Rn. 119. Gemäss der Rechtsprechung des BGer ist es zur Vermeidung negativer Kompetenzkonflikte geboten, auch in Fällen ohne engen Bezug zur Schweiz eine Schweizer Zuständigkeit zu bejahen (BGE 141 IV 205, E. 5.2).

137 GLESS, Rn. 120 ff. m.w.H.

138 GLESS, Rn. 120; EICKER, § 3 N 3.

139 Siehe vorn, III.1.1.

140 Bei Unterlassungen gilt der Ort, wo der Täter hätte handeln müssen, als Handlungsort. Beim Versuch gilt der Ort, wo der Versuch ausgeführt wird, und der Ort, wo der Erfolg nach der Vorstellung des Täters hätte eintreten sollen, als Handlungsort (Art. 8 Abs. 2 StGB).

wendungsrecht ist der Handlungsort[141]. Bei Delikten, deren Ausführungshandlungen in einem Äussern, Verbreiten, Darstellen oder Zugänglichmachen bestehen (Datenweitergabe- oder Kommunikationsdelikte), ist der Aufenthaltsort des Täters im Moment der physischen oder digitalen Offenbarungshandlung massgebend. Im Kontext von Netzwerken ist dies die Eingabe des Übermittlungs- bzw. Abspeicherungsbefehls, mit dem die Daten auf den Bereich der Festplatte eines Rechners (Web-Server, Mail-Server, Cloud-Server) transferiert werden, die von mindestens einem unbefugten Dritten eingesehen werden kann[142]. Findet diese Handlung innerhalb der Schweiz statt, ist die Berufsgeheimnisverletzung somit in der Schweiz verfolgbar. Befindet sich allerdings ein Cloud-Provider als Hilfsperson bei der Offenbarungshandlung im Ausland, ist die entsprechende Tathandlung im Ausland zu verorten. In solchen Fällen ist eine Anknüpfung nur am Erfolgsort möglich[143]. Der Erfolg von Art. 321 StGB besteht in der Kenntnisnahme durch einen beliebigen unberechtigten Dritten. Erfolgsort im Sinn von Art. 8 Abs. 1 StGB ist damit der Ort, an dem die Kenntnisnahme stattfindet. Hält sich der unberechtigte Dritte im Zeitpunkt der Kenntnisnahme im Ausland auf, ist eine Anknüpfung nach dem Territorialitätsprinzip nicht möglich (Art. 3 i.V.m. Art. 8 StGB). Im Anknüpfungskriterium des Erfolgs liegt etwas Zufälliges, weil der Aufenthaltsort des unbefugten Dritten bei der Kenntnisnahme beliebig ist[144]. Eine Strafhoheit nach dem Territorialitätsprinzip ist bei einem Schweizer Anwalt bzw. einer Schweizer Anwältin, der bzw. die (Haupt-)Geheimnisträger ist, damit in der Regel gegeben[145],

---

141 DYENS, 159 ff.; MUGGLI, 187 ff.; BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 1 f.; SCHWARZENEGGER, ZStrR 2000, 117 ff. je m.w.H. Vgl. zum Primat des Handlungsortes auch Art. 31 StPO.

142 BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 4 ff.; SCHWARZENEGGER, ZStrR 2000, 118 f. m.w.H.

143 Zum Erfolgsort siehe BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 9 ff.; SCHWARZENEGGER, ZStrR 2000, 119 ff. m.w.H.

144 Kritisch zu diesem Punkt BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 10 f.

145 Ausnahmsweise wäre eine solche zu verneinen, wenn sich der Anwalt im Moment der Offenbarung physisch im Ausland befindet.

so dass die Strafverfolgung im Inland unproblematisch erscheint. Da aber beim (Haupt-)Geheimnisträger der Vorsatz kaum zu bejahen sein wird[146], bleibt er aus materiellen Gründen straflos.

Alternativ lässt sich die schweizerische Strafhoheit auf das passive Personalitätsprinzip gründen (Art. 7 StGB)[147]. Wenn ein Schweizer Geheimnisherr von der Tat betroffen ist, kann eine Auslandtat in der Schweiz verfolgt werden, sofern die Berufgeheimnisverletzung auch am ausländischen Begehungsort strafbar ist, der Täter sich in der Schweiz befindet oder ihr wegen dieser Tat ausgeliefert wird und nach schweizerischem Recht die Tat die Auslieferung zulässt[148], der Täter jedoch nicht an den Staat des Begehungsortes ausgeliefert wird (vgl. Art. 7 Abs. 1 StGB)[149]. Das grösste Hindernis einer Strafverfolgung von solche Auslandtaten in der Schweiz besteht darin, dass sich der im Ausland handelnde Täter kaum freiwillig in die Schweiz begeben wird bzw. die Auslieferung durch den ausländischen Staat scheitert, weil er eigene Staatsbürger nicht ausliefert oder der Begehungsort nicht festgestellt werden kann.

Als Resultat ist festzuhalten, dass nicht alle Berufsgeheimnisverletzungen, die im Ausland begangen werden, unter die Schweizer Strafhoheit fallen. In den beschriebenen Fällen ohne Handlungs- oder Erfolgsort in der Schweiz erscheint der Geheimnisschutz durch die Schweizer Strafverfolgungsbehörden deshalb eingeschränkt. Eine Verfolgung nach dem passiven Personalitätsprinzip ist von mehreren einschränkenden Voraussetzungen abhängig. Andererseits ist darauf hinzuweisen, dass eine Verletzung des Berufsgeheimnisses in den meisten ausländischen Staaten ebenfalls strafbar ist und es dem Ge-

146 Siehe vorn, III.1.3.

147 Zum passiven Personalitätsprinzip weiterführend BSK-Strafrecht I, POPP/KESHELAVA, StGB vor 3 N 21; StGB 7 N 1 ff. m.w.H.

148 Die Voraussetzung der Mindesthöchststrafe von einem Jahr Freiheitsstrafe ist bei Art. 321 StGB erfüllt, siehe Art. 35 Abs. 1 IRSG.

149 Weitere Einschränkungen gelten, wenn der Geheimnisherr nicht Schweizer ist, vgl. Art. 7 Abs. 2 StGB.

heimnisherrn offen steht, jederzeit bei einer ausländischen Strafverfolgungsbehörde Strafanzeige zu erstatten. Die Schweizer Strafverfolgungsbehörden können ausserdem jederzeit ein Ersuchen um stellvertretende Strafrechtspflege stellen[150].

[150] Art. 88 f. IRSG.

2. Verletzung einer beruflichen Schweigepflicht

2.1 Objektiver Tatbestand

a) Täterkreis und Angriffsobjekt

Art. 35 DSG stellt die unbefugte Bekanntgabe geheimer, besonders schützenswerter Personendaten sowie die Bekanntgabe von Persönlichkeitsprofilen, unter Strafandrohung. Da das Geheimnis kumulativ zur besonderen datenschutzrechtlichen Qualifikation der Daten gegeben sein muss, ist das Angriffsobjekt enger definiert als bei Art. 321 StGB[151]. Besonders schützenswerte Personendaten i.S.v. Art. 3 lit. c DSG sind Daten, über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit, Daten über Massnahmen der sozialen Hilfe, sowie Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Persönlichkeitsprofile werden in Art. 3 lit. d DSG als eine Zusammenstellung von Daten definiert, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Diese besonders schützenswerten Personendaten oder Persönlichkeitsprofile müssen zudem geheim sein. Geheim sind Daten, wenn sie relativ unbekannt sind und der Geheimnisherr ein berechtigtes Interesse an ihrer Geheimhaltung hat[152].

Art. 35 DSG ist als echtes Sonderdelikt konzipiert. Tauglicher Täter ist nur, wer einen Beruf ausübt, der die Kenntnis geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile erfordert und solche Daten tatsächlich bei der Berufsausübung wahrgenommen hat[153]. Diese Bestimmung erfasst daher nur bestimmte Berufs-

151 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 1.

152 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 9, m.w.H.

153 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 40.

gruppen[154]. Strafbar sind weiter auch Personen, welche für einen Berufsausübenden als Hilfspersonen oder auszubildende Personen die fraglichen Daten bekannt geben[155]. Dabei gelten die gleichen Kriterien wie bei Art. 321 Ziff. 1 Abs. 1 StGB[156].

b) Tathandlung

Strafbar ist die Bekanntgabe von geheimen, besonders schützenswerter Personendaten. Art. 3 lit. f DSG definiert die Bekanntgabe als das Zugänglichmachen von Daten. Beispielhaft werden vom Gesetz die Weitergabe, das Einsichtgewähren oder das Veröffentlichen von Daten genannt[157]. Erfasst ist jeder Vorgang, der es Dritten ermöglicht, vom Inhalt der Daten Kenntnis zu nehmen[158].

2.2 Subjektiver Tatbestand

Subjektiv ist Handeln mit Vorsatz erforderlich, wobei Eventualvorsatz genügt. Es reicht aber, wenn der Täter mit der Möglichkeit rechnet, geheime, besonders schützenswerten Personendaten zu offenbaren und diese Möglichkeit in Kauf nimmt (Art. 12 Abs. 2 StGB)[159].

2.3 Strafantrag

Zum Stellen eines Strafantrags berechtigt ist nach einem Teil der Lehre der Geheimnisherr[160], also diejenige Person, welche die fraglichen

154 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 8; Der Gesetzgeber nannte Sozialarbeiter, Ehevermittler und Psychologen als Beispiele (BBl 1988 II 413, 485) wobei Psychologen seit 1. April 2013 ebenfalls von Art. 321 Ziff. 1 StGB erfasst sind.

155 BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.6; BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 10.

156 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 12 m.w.H.

157 SHK-DSG, RUDIN, DSG 3 N 41.

158 BSK-DSG/BGÖ, BLECHTA, DSG 3 N 77; BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 15.

159 Siehe BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 42.

160 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 67.

Daten dem Geheimnisträger zur Berufsausübung mitgeteilt hat. Gemäss anderer Ansicht ist die datenschutzrechtlich betroffene Person (vgl. Art. 3 lit. b DSG) antragsberechtigt, d.h. diejenige Person, auf die sich die Personendaten beziehen[161]. Geheimnisherr und betroffene Person müssen nicht identisch sein. So kann z.B. ein Sozialarbeiter von der betreuten Person (Geheimnisherr) Informationen erfahren haben, die eine strafrechtliche Verfolgung ihres Partners (betroffene Person) betreffen. Da Art. 35 DSG eine Lücke im beruflichen Geheimnisschutz schliessen soll[162], erscheint es sachgerecht, analog zur Verletzung des Berufsgeheimnisses nur dem Geheimnisherrn das Antragsrecht zuzugestehen.

2.4 Konkurrenz

Durch eine Offenbarung bzw. Bekanntgabe von Informationen können sowohl Art. 321 StGB als auch Art. 35 DSG erfüllt sein, wenn der Täter beide Sondereigenschaften auf sich vereinigt. Die Lehre geht davon aus, dass zwischen Art. 321 StGB und Art. 35 DSG unechte Idealkonkurrenz besteht, die Verletzung einer beruflichen Schweigepflicht wird also durch die Verletzung eines Berufsgeheimnisses konsumiert[163].

---

161 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 4 und DSG 34 N 22.

162 BBl 1988 II 413, 485.

163 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 74; SHK-DSG, PÄRLI, DSG 35 N 12; Siehe aber ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 17, gemäss dem Art. 35 DSG bloss «subsidiär» zur Anwendung kommt.

IV. Datenschutzrecht

1. Vorbemerkungen

Die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte muss in Übereinstimmung mit den Vorgaben des Datenschutzrechts erfolgen, wenn die Anbieter dieser Dienste Personendaten im Sinn des Datenschutzrechts bearbeiten. Fehlt es an einer Bearbeitung von Personendaten, namentlich weil die von den Anwältinnen und Anwälten übermittelten Daten schon bei diesen verschlüsselt werden[164], kommt das Datenschutzrecht auf die Tätigkeit der Anbieter von Cloud-Diensten nicht zur Anwendung.

Ist eine Bearbeitung von Personendaten gegeben, stellt sich die Frage nach dem anwendbaren Recht. Im Vordergrund stehen dabei das schweizerische Datenschutzrecht (DSG) und die Datenschutz-Grundverordnung der EU (DSGVO). Werden Personendaten ausländischer Klientinnen und Klienten bearbeitet, kann diese Bearbeitung durch die Anbieter von Cloud-Diensten aber auch einer anderen Rechtsordnung unterstehen, wenn deren Bestimmungen aufgrund der Regeln des jeweils anwendbaren internationalen Privatrechts Anwendung finden. Das vorliegende Gutachten beschränkt sich allerdings auf die Beurteilung nach dem geltenden DSG und dem Entwurf für ein revidiertes DSG (E-DSG) sowie nach der DSGVO.

Gegenstand dieses Gutachtens ist die Frage, unter welchen Voraussetzungen und in welchen Konstellationen die Tätigkeit von schweizerischen Anwältinnen und Anwälten der DSGVO untersteht. Aufzuzeigen ist deshalb nur, dass die DSGVO in vielen Konstellationen zur Anwendung kommen kann und wie die Nutzung von Cloud-Diensten durch schweizerische Anwältinnen und Anwälte auszugestalten ist, damit die Vorgaben der DSGVO eingehalten werden,

[164] Siehe vorn, II.3.2.

wenn diese zur Anwendung gelangen sollte. Fragen der Vollstreckung und Aufsicht werden ebenfalls ausgeklammert[165].

2. Anwendbarkeit

2.1 Anwendbares Recht

a) Schweizerisches Datenschutzgesetz (DSG)

Die Bearbeitung von Personendaten durch Anwältinnen und Anwälte in der Schweiz und die Nutzung von Cloud-Diensten zu diesem Zweck untersteht grundsätzlich dem DSG. Dies jedenfalls, soweit ein rein inländischer Sachverhalt vorliegt, wenn also Schweizer Anwältinnen und Anwälte die Daten von Schweizer Klienten unter Beizug von Schweizer Cloud-Providern bearbeiten. Weist ein Sachverhalt hingegen einen qualifizierten Auslandsbezug auf, kann aufgrund des IPRG ausländisches Recht zur Anwendung kommen. Zwingend ist dies allerdings nicht, weil das IPRG auch auf das Schweizer DSG verweisen kann. Namentlich hat die betroffene Person – bspw. eine ausländische Klientin – nach Art. 139 Abs. 3 i.V.m. Abs. 1 lit. b IPRG die Wahl, ihre Ansprüche aus Datenschutzrecht dem Recht des Staates zu unterstellen, in welchem der Urheber der Verletzung, hier also die Schweizer Anwältin oder der Schweizer Anwalt, die Niederlassung oder den gewöhnlichen Aufenthalt hat.

b) Datenschutz-Grundverordnung (DSGVO)

i. Extraterritoriale Anwendbarkeit der DSGVO

Die DSGVO folgt dem Niederlassungs- und Marktortprinzip (Art. 3 Abs. 2 DSGVO): Unter die DSGVO fallen (i) das Verarbeiten von Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union, (ii) das An-

[165] Siehe dazu: BENHAMOU/JACOT-GUILLARMOD, digma 2018, *passim*; HOEREN, EuZ 2018, *passim;* AZZI, JIPITEC 2018, 132.

bieten von Waren oder Dienstleistungen an Personen in der EU sowie (iii) die Verhaltensbeobachtung von Personen, die sich in der EU aufhalten.

Mit dem Marktortprinzip kommt die DSGVO einer grundrechtlichen Schutzpflicht gegenüber EU-Bürgern nach und will ein Level-Playing-Field für den EU Markt schaffen[166]. Die Tätigkeit von Schweizer Anwältinnen und Anwälten kann durchaus unter die DSGVO fallen[167], etwa wenn sie ihr Angebot auf Klienten aus dem Raum der EU ausrichten. Der Begriff des «Ausrichtens» ist gemäss ErwG 23 DSGVO in Anlehnung an die Rechtsprechung des EuGH auszulegen[168], weshalb die Abrufbarkeit einer Website aus der EU für sich genommen nicht genügt[169]. Das Angebot muss vielmehr einen internationalen Charakter haben, was sich insb. aus der Verwendung einer ausländischen oder internationalen Toplevel Domain, aus Anfahrtsbeschreibungen für ausländische Kunden oder aus der Werbung mit Kundenbewertungen aus EU-Staaten ergeben kann[170].

Zudem muss nach ErwG 22 DSGVO eine Auftragsdatenverarbeitung (siehe dazu hinten, IV.3.2a)) in der EU den Vorgaben der DSGVO genügen, gleich ob die Verarbeitung in der EU stattfindet oder nicht. Dies bedeutet aber nicht, dass jede Inanspruchnahme eines Auftragsdatenverarbeiters in der EU zur Anwendbarkeit der DSGVO für Schweizer Unternehmen führt. Der Anwendungsbereich der DSGVO

166 ENÖCKL, in: Sydow, DSGVO 3 N 17.

167 STEIGER, AwR 2018, 206.

168 Siehe EuGH, Urteil vom 7. Dezember 2010, C-585/08 und C-144/09, Pammer/Alpenhof zur Auslegung des Begriffs des Ausrichtens einer Tätigkeit nach Art. 15 Abs. 1 lit. c Brüssel-I VO. Diese Rechtsprechung ist für Schweizer Unternehmen im euronationalen Verbrauchergeschäft bereits aufgrund von Art. 15 Abs. 1 LugÜ von Bedeutung (siehe ZERDICK, in: Ehmann/Selmayr, DSGVO 3 N 19; GEORGE/TAMÒ, 39 f.; AZZI, JIPITEC 2018, 129).

169 EuGH, Urteil vom 7. Dezember 2010, C-585/08 und C-144/09, Pammer/Alpenhof, Rn. 69; HOEREN, EuZ 2018, 162 f.; PRAZ, AJP 2018, 610.

170 EuGH, Urteil vom 7. Dezember 2010, C-585/08 und C-144/09, Pammer/Alpenhof, Rn. 83.

ergibt sich aus dem Wortlaut von Art. 3 DSGVO. Ein Erwägungsgrund kann den Verordnungstext erläutern und präzisieren, nicht aber selbst Pflichten auferlegen[171]. Adressaten der DSGVO sind primär in der Union ansässige Unternehmen und ErwG 22 stellt klar, dass diese für die Einhaltung der DSGVO verantwortlich bleiben, selbst wenn sie eine Auftragsdatenverarbeitung aus der EU auslagern[172].

Die DSGVO ist supranationales Recht der EU. Obwohl sie als EU-Verordnung direkt anwendbar ist, erreicht sie keine Vollharmonisierung[173]. Vielfach werden gewisse Tätigkeiten verboten und es wird dem nationalen Gesetzgeber mittels sog. Öffnungsklauseln ermöglicht, von den Vorschriften der DSGVO abzuweichen[174]. Es stellt sich daher die Frage, welches nationale Umsetzungsrecht auf einen grenzüberschreitenden Sachverhalt anzuwenden ist. Diese Frage ist schon im Verhältnis der Mitgliedsstaaten untereinander ungeklärt, weil die DSGVO keine Kollisionsregeln enthält[175]. Dies gilt erst recht für die extraterritoriale Anwendung der DSGVO in der Schweiz.

---

171 EuGH, Urteil vom 13. Juli 1989, C-215/88, *Casa Fleischhandel*, Rn. 31.

172 PRAZ, AJP 2018, 610; PILTZ, in: Gola, DSGVO 3 N 5: «Abs. 2 regelt Konstellationen, in denen der Verantwortliche oder Auftragsverarbeiter, zumindest dem Wortlaut nach, gar nicht in der EU niedergelassen ist». Siehe auch VASELLA, digma 2017, *passim*, jedoch mit anderer Begründung.

173 LAUE, ZD 2016, 464.

174 STEIGER, AwR 2018, 205. So dürfen z.B. Informationen über strafrechtliche Verurteilungen nur unter behördlicher Aufsicht bearbeitet werden oder wenn das Recht der Mitgliedsstaaten oder der EU dies vorsieht (Art. 10 DSGVO). Auch wenn dies kein Verarbeitungsverbot solcher Daten statuiert, sondern lediglich einen «verantwortungsvollen» Umgang mit solchen Daten sicherstellen soll (SCHIFF, in: Ehmann/Selmayr, DSGVO 10 N 1), wurde z.B. im irischen Recht klargestellt, dass Daten über strafrechtliche Verurteilungen für die Erbringung von Rechtsdienstleistungen oder die Durchsetzung von Rechtsansprüchen verarbeitet werden dürfen (Art. 55(1)(b) Irish Data Protection Act 2018).

175 PILTZ, in: Gola, DSGVO 3 N 3 und 38 ff.; LAUE, ZD 2016, 464, mit der bemerkenswerten Feststellung, dass dies im Zeitdruck des Gesetzgebungsverfahrens wohl vergessen ging, da ursprünglich eine Vollharmonisierung geplant war.

Ob eine Anwaltskanzlei ihre Tätigkeit auf die EU ausrichtet, ist im Einzelfall zu prüfen. Dabei ist nicht zuletzt auf den Web-Auftritt der Kanzlei abzustellen. Namentlich grössere Anwaltskanzleien richten ihr Angebot regelmässig (auch) auf Klienten in der EU aus. Aber auch kleinere Kanzleien können dieses Kriterium erfüllen, wenn sie z.B. in einem Newsletter auf Rechtsentwicklungen mit besonderer Relevanz für Klienten in der EU aufmerksam machen. Der Zielsetzung der DSGVO entsprechend, fallen nur diejenigen Daten, die aufgrund einer Ausrichtung auf den EU-Markt bearbeitet werden, unter das europäische Recht[176]. Folglich müssen die Bestimmungen der DSGVO nur für die Daten europäischer Klienten beachtet werden.

ii. Anwendbarkeit aufgrund des IPRG

Wird ein Verfahren vor einem Schweizer Gericht anhängig gemacht, bestimmt sich das anwendbare Recht nach dem IPRG. Bei einem Verfahren vor einem ausländischen Gericht, würde sich das anwendbare Recht nach dem internationalen Privatrecht der jeweiligen *lex fori* bestimmen. Nachfolgend kann nur erstere Konstellation abgedeckt werden. Fragen der internationalen Zuständigkeit werden ebenso ausgeklammert.

Das Datenschutzrecht dient dem Schutz der Persönlichkeit der betroffenen Personen (Art. 1 DSG). Klagt die durch eine Datenverarbeitung in ihrer Persönlichkeit verletzte Person vor Schweizer Gerichten, so bestimmt sich das anwendbare Recht nach Art. 139 Abs. 3 i.V.m. Art. 139 Abs. 1 IPRG: Zur Anwendung kommt nach Wahl des Geschädigten (i) das Recht des Staates, in dem die geschädigte Person ihren gewöhnlichen Aufenthalt hat, sofern der Schädiger mit einem Schadenseintritt in diesem Land rechnen musste (lit. a), (ii) das Recht am Ort der Niederlassung oder des gewöhnlichen Aufenthalts des Schädigers (lit. b) oder (iii) das Recht am Erfolgsort, sofern der Schä-

[176] STEIGER, AwR 2018, 206. Letztlich sind noch sehr viele Fragen zum Marktortprinzip ungeklärt.

diger mit einem Erfolgseintritt in diesem Staat rechnen musste (lit. c). Nach der Lehre kann das Recht am Aufenthaltsort des Geschädigten gewählt werden, selbst wenn noch kein nachweisbarer Erfolg eingetreten ist[177]. Das Recht des gewöhnlichen Aufenthaltsortes kann daher insb. für Unterlassungsklagen angerufen werden, bei denen ein Erfolgseintritt oft erst befürchtet wird[178]. Das Recht am Erfolgsort kann hingegen erst nach Erfolgseintritt gewählt werden. Als Erfolgsort gilt der Ort, an dem die erste unmittelbare Einwirkung auf das Rechtsgut stattgefunden hat[179]. Im Datenschutzrecht ist dies der Ort an dem die Daten zugänglich werden, an dem sich die verpönte Wirkung der Datenbearbeitung zu entfalten beginnt oder der Ort, an dem sich die betroffene Person zum Eingriffszeitpunkt aufhält[180]. Sowohl das Recht am Erfolgsort als auch das Recht am gewöhnlichen Aufenthaltsort können nur gewählt werden, wenn diese Anknüpfungspunkte für den Schädiger vorhersehbar waren. Da ein Erfolgseintritt am gewöhnlichen Aufenthaltsort der betroffenen Person in der Regel vorhersehbar ist[181], begrenzt die Vorhersehbarkeit vor allem die Wahl des an den Erfolgsorten geltenden Rechts.

Die Wahl kann frühestens mit dem anspruchsbegründenden Ereignis erfolgen[182]. Umstritten ist, ob die Wahl der betroffenen Person unwiderruflich ist[183]. Eine akzessorische Anknüpfung der Rechtswahl an

177 BSK-IPRG, DASSER, IPRG 139 N 11; PASSADELIS, Rz. 6.30; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 25, mit der einleuchtenden Begründung, dass ansonsten die Wahlmöglichkeit von Art. 139 Abs. 1 lit. a in derjenigen von lit. c aufgehen würde, da auch am Aufenthaltsort ein Erfolgsort bestehen kann.

178 Siehe ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 25.

179 BGE 125 III 103 E. 2b; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 20; THALMANN, sic! 2007, 339; BÜHLMANN/REINLE, digma 2017, 10.

180 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 22.

181 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 26; BÜHLMANN/REINLE, digma 2017, 10.

182 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 15.

183 Siehe ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 14.

das Vertragsstatut, z.B. ein Mandatsverhältnis, wird mit Blick auf das Schutzziel der Norm von der h.L. zu Recht abgelehnt[184].

Auf eine persönlichkeitsverletzende Bearbeitung von Personendaten in einer Cloud findet somit das Recht am Sitz der Anwältin bzw. des Anwalts, das Recht am Erfolgsort oder das Recht am Aufenthaltsort der betroffenen Person Anwendung, sofern die Anwältin bzw. der Anwalt mit einer Persönlichkeitsverletzung in diesem Land rechnen musste. Da mit einem Erfolgseintritt am gewöhnlichen Aufenthaltsort des Klienten in der Regel zu rechnen ist, kann sich die Anwendung der DSGVO für Anwältinnen und Anwälte mit Klienten in der EU auch aus dem schweizerischen IPRG ergeben. Diesem Risiko kann nicht mit einer Rechtswahl begegnet werden, da diese erst nach Eintritt der Persönlichkeitsverletzung möglich ist[185].

Liegt der Aufenthaltsort des Klienten in einem EU-Staat, stellt sich die Frage, wie weit eine allfällige Rechtswahl reichen würde. Diese umfasst grundsätzlich alle Bestimmungen, die nach dem gewählten Recht auf den Sachverhalt anwendbar sind (Art. 13 Abs. 1 IPRG). Dazu gehören sowohl nationales als auch supranationales Recht[186]. Eine Rechtswahl des Klienten kann sich folglich nicht nur auf die DSGVO beziehen. Zur Anwendung käme sowohl die DSGVO als auch das nationale, die DSGVO umsetzende Recht am Aufenthaltsort des Klienten.

2.2 Bearbeiten von Personendaten

a) Allgemein

Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare (Art. 3 lit. a DSG) bzw. identifizierte oder identifi-

184 BSK-IPRG, DASSER, IPRG 139 N 22 und N 48; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 16; THALMANN, sic! 2007, 340.

185 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 15; PASSADELIS, Rz. 6.31.

186 BSK-IPRG, MÄCHLER-ERNE/WOLF-METTIER, IPRG 13 N 7.

zierbare Person (Art. 4 Abs. 1 DSGVO) beziehen. Für die Trennung von Personen- und Sachdaten ist damit entscheidend, ob eine Person bestimmbar bzw. identifizierbar ist.

Auch wenn die DSGVO und das DSG in der deutschen Sprachversion unterschiedliche Begriffe verwenden, liegt beiden das Konzept der relativen Bestimmbarkeit zu Grunde[187]. Die Bestimmbarkeit kann sich zwar aus der Kombination einer Angabe mit zusätzlichen Informationen ergeben, es genügt dabei aber nicht schon jede theoretische Möglichkeit der Identifizierung. Die Bestimmbarkeit ist aber gegeben, wenn nach der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass ein Interessent den Aufwand auf sich nehmen würde, um die Person zu bestimmen, wobei der Stand der Technik und die technischen Entwicklungsmöglichkeiten zu berücksichtigen sind[188]. Umstritten ist dabei, ob auf die Perspektive des jeweiligen Bearbeiters abzustellen ist[189] oder ob die Mittel entscheidend sind, die ein Dritter zur Verfügung hätte[190]. Würde letzterer Auffassung gefolgt, wären die Kriterien des Interesses und des Aufwands allerdings bedeutungslos, weil völlig unklar bliebe, nach wessen Beurteilungshorizont diese zu bestimmen wären. Im Grundsatz ist deshalb auf die Perspektive des jeweiligen Bearbeiters abzustellen. Immerhin sind die Interessen, Zusatzinformationen und Informationsmöglichkeiten eines Dritten ausnahmsweise zu berücksichtigen, wenn diese dem die Daten übermittelnden Bearbeiter bekannt waren oder hätten bekannt sein müssen[191] oder wenn der die Daten übermittelnde Bearbeiter indirekt auf diese Mittel zugreifen kann[192]. Ein Daten übermittlender

187 SCHREIBER, in: Plath, DSGVO 4 N 9 ff.; BSK-DSG/BGÖ, BLECHTA, DSG 3 N 10; SHK-DSG, RUDIN, DSG 3 N 12; SPINDLER/SCHMECHEL, JIPITEC 2016, 169.

188 BGE 136 II 508, E. 3.2; BGer 4A_365/2017, Urteil vom vom 26. Februar 2018, E. 5; EuGH, Urteil vom 19. Oktober 2016, C-582/14, Breyer, Rn. 46 f.; DSGVO, ErwG 26.

189 SCHREIBER, in: Plath, DSGVO 4 N 9 ff.

190 KLABUNDE, in: Ehmann/Selmayr, DSGVO 4 N 13; BSK-DSG/BGÖ, BLECHTA, DSG 3 N 11.

191 PROBST, AJP 2013, 1435; ähnlich: ROSENTHAL, in: Rosenthal/Jhöri, DSG 3 N 26 ff.

192 Siehe auch EuGH, Urteil vom 19. Oktober 2016, C-582/14, Breyer, Rn. 46 f.

Bearbeiter untersteht daher selbst dann dem Datenschutzrecht, wenn er aus den Daten selbst keine Personen identifizieren kann, die Daten aber an einen Bearbeiter übermittelt, der über diese Möglichkeit verfügt und an einer Identifizierung auch interessiert ist[193].

Da der Personenbezug relativ ist, muss für jede involvierte Person gesondert geprüft werden, ob aus ihrer Sicht Personendaten vorliegen. Damit ist ohne weiteres denkbar, dass die in Frage stehenden Daten für die Anwältinnen und Anwälte als Personendaten zu qualifizieren sind, nicht aber für die Anbieter von Cloud-Diensten. Dies ist namentlich der Fall, wenn die Verschlüsselung vor der Übertragung der Daten stattfindet (siehe vorn, II.3.2) und die Cloud-Provider ihre Dienste erbringen, ohne auf die Daten der Klienten zugreifen zu können[194]. Dies ist aber grundsätzlich nur der Fall, wenn der Dienst auf die blosse Datenspeicherung beschränkt bleibt[195] (siehe vorn, II.2.3). Anderes gilt bei der Nutzung eines SaaS-Dienstemodells, bei welchem der Cloud-Provider die Softwareapplikationen nur auf im Klartext gespeicherten, also unverschlüsselten Daten ausführen kann (siehe vorn, II.3.3). In dieser Konstellation hat der Cloud-Provider Zugriff auf die Klientendaten.

b) Besondere Kategorien von Daten

Anwältinnen und Anwälte können verschiedene Kategorien von Daten auf den Servern von Cloud-Providern speichern und bearbeiten. Für besonders schützenswerte Personendaten bzw. besondere Kategorien personenbezogener Daten[196] gelten indes besondere Regeln.

---

193 BGE 136 III 508 E. 3.4.

194 STRAUB, AJP 2014, 913; STAIGER, 203; RÜPKE/VON LEWINSKI/ECKHARDT, 142. Zur vergleichbaren Situation im Strafrecht: WOHLERS, digma 2017, 115.

195 STRAUB, AJP 2014, 913.

196 Das DSG verwendet den Term «besonders schützenswerte» (Art. 3 lit. c DSG) während die DGSVO von «besonderen Kategorien» spricht (Art. 9 DSGVO). Der besondere Schutz dieser Daten wird aber zumindest teilweise bereits von der Konvention-108 vorgeschrieben (Art. 6 Konvention-108).

Dies gilt für Daten über die Rasse oder Ethnie, weltanschauliche und politische Ansichten, gewerkschaftliche Tätigkeiten sowie über die Gesundheit und Intimsphäre. In der EU gilt dies auch für genetische und biometrische Daten, in der Schweiz auch für Daten über Massnahmen der Sozialhilfe sowie solche über administrative und strafrechtliche Verfolgung und Sanktionen. Anderes gilt für Daten über eine strafrechtliche Verfolgung in der EU, die nach der DSGVO nur unter behördlicher Aufsicht verarbeitet werden dürfen (Art. 10 DSGVO)[197].

Nach dem DSG kann die Bearbeitung von besonders schützenswerten Personendaten durch Gesetz, Einwilligung oder überwiegende Interessen gerechtfertigt werden (Art. 13 Abs. 1 DSG). Stützt sich die Bearbeitung auf eine Einwilligung, muss sie ausdrücklich erfolgen (Art. 4 Abs. 5 DSG)[198], stützt sie sich auf eine Interessenabwägung, ist der Sensitivität der Daten bei dieser Abwägung Rechnung zu tragen[199]. Besonders schützenswerte Personendaten dürfen zudem nicht ohne Rechtfertigungsgrund bekannt gegeben werden (Art. 12 Abs. 2 lit. c DSG)[200].

Nach der DSGVO dürfen besondere Kategorien von personenbezogenen Daten grundsätzlich nicht verarbeitet werden. Anderes gilt nur, wenn ein besonderer Ausnahmetatbestand vorliegt. Im Vordergrund stehen für Anwältinnen und Anwälte die Zulässigkeit aufgrund einer Einwilligung (Art. 9 Abs. 2 Bst. a DSGVO) und die Erforderlichkeit der Verarbeitung im Zusammenhang mit der Geltend-

---

197 Die abschliessende Aufzählung ist weitgehend aleatorisch und Versuche überzeugende, allgemein akzeptierte Kriterien für die besondere Sensitivität zu erarbeiten, sind bis anhin erfolglos geblieben (siehe dazu schon: SIMITIS, FS Pedrazzini, 475; SHK-RUDIN, DSG 3 N 21, der die Auswahl als «willkürlich, antiquiert und unvollständig» bezeichnet).

198 SHK-DSG, BAERISWYL, DSG 4 N 71; ROSENTHAL, in: Rosenthal/Jhöri, DSG 4 N 83.

199 BSK-DSG/BGÖ, RAMPINI, DSG 13 N 23; ROSENTHAL, Datenschutz im IT-Outsourcing, 197.

200 ROSENTHAL, in: Rosenthal/Jhöri, DSG 12 N 44 f; kritisch: SHK-DSG, WERMELINGER, DSG 12 N 8.

machung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 9 Abs. 2 Bst. f DSGVO). Eine Bearbeitung gestützt auf überwiegende Interessen oder andere Tatbestände von Art. 6 DSGVO wird von der h.L. abgelehnt, weil Art. 9 DSGVO als *lex specialis* zu Art. 6 DSGVO zu verstehen sei[201]. Es bestehen aber überzeugende Gründe, auch bei besonderen Kategorien von Daten eine Verarbeitung gestützt auf eine Interessenabwägung zuzulassen[202]. Für Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO entspricht dies sogar der h.L.[203].

2.3 Zwischenfazit

Auf die Nutzung von Cloud-Diensten durch Schweizer Anwältinnen und Anwälte können – je nach Ausrichtung und Klientschaft – die Bestimmungen des DSG oder diejenigen der DSGVO anwendbar sein. Die nachfolgende datenschutzrechtliche Beurteilung muss deshalb die Vorgaben beider Regelungen beachten. Soweit Anwältinnen und Anwälte besondere Kategorien von Personendaten bearbeiten, sind die erhöhten Anforderungen von DSG und DSGVO einzuhalten.

---

201 Explizit immerhin: SCHULZ in: Gola, DSGVO 9 N 5; KAMPERT, in: Sydow, DSGVO 9 N 63. Siehe auch LAUE/NINK/KREMER, § 2 N 60; SCHIFF, in: Ehmann/Selmayr, DSGVO 9 N 10 f.

202 ROBRAHN/BREMERT, ZD 2018, 295; siehe auch SCHULZ, in: Gola, DSGVO 9 N 5 f., nach dem nur eine Bearbeitung auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO ausscheidet, die anderen Erlaubnistatbestände jedoch angerufen werden können. Einen Grund Art. 9 DSGVO grosszügig auszulegen kann man darin sehen, dass der Kritik an Art. 9 DSGVO regelmässig dessen symbolische Bedeutung entgegengehalten wird (vgl. SCHIFF, in: Ehmann/Selmayr, DSGVO 9 N 1 ff.). Wenn es sich bei Art. 9 DSGVO um symbolische Gesetzgebung handelt, erscheint eine streng am Wortlaut orientierte Auslegung nicht angezeigt.

203 Art. 10 DSGVO statuiert hiernach kein Verarbeitungsverbot, sondern will lediglich einen «verantwortungsvollen» Umgang mit Daten über strafrechtliche Verurteilungen sicherstellen (SCHIFF, in: Ehmann/Selmayr, DSGVO 10 N 1; vgl. KAMPERT, in: Sydow, DSGVO 10 N 5; GOLA, in: Gola, DSGVO 10 N 6 f.).

Das DSG und die DSGVO sind auf die Nutzung von Cloud-Diensten durch Schweizer Anwältinnen und Anwälte allerdings nur anwendbar, wenn die Daten für den Cloud-Provider als Personendaten zu qualifizieren sind. Dies ist nicht der Fall, wenn die Daten vor der Übertragung auf den Cloud-Provider hinreichend verschlüsselt werden und der Cloud-Provider keinen Zugriff auf den Schlüssel hat. Anderes gilt, wenn der Cloud-Provider, insb. bei einem SaaS-Dienstemodell, die Software für die Kanzlei in einer virtuellen Maschine betreibt und damit Zugang zu den im Dokument gespeicherten Daten im Klartext hat oder haben kann (siehe vorn, II.3.3). Datenschutzrechtlich relevant und nachfolgend zu untersuchen ist nur diese zweite Konstellation.

3. Auftragsdatenbearbeitung

3.1 Nach dem DSG

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz auf Dritte übertragen werden. Dies ist bei der Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte der Fall. Eine solche Auftragsdatenbearbeitung ist zulässig, wenn die Daten vom Dritten nur so bearbeitet werden, wie der Auftraggeber es selbst tun dürfte (Art. 10a Abs. 1 lit. a DSG) und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet (Art. 10a Abs. 1 lit. b DSG)[204]. Der Auftraggeber muss sich zudem vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG).

a) Übertragung durch Vereinbarung

Das Bearbeiten von Personendaten durch die Anbieter von Cloud-Diensten beruht auf einer Vereinbarung zwischen den Anwältinnen

[204] WIDMER, digma 2014, 28; ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 43; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 3; SHK-DSG, BAERISWYL, DSG 10a N 18; WAGNER/ZWIRNER, 170 f.

und Anwälten bzw. deren Kanzlei und dem Dienstleister. Der Cloud-Vertrag ist ein Innominatvertrag mit Dauerschuldcharakter, der je nach Ausgestaltung der Dienste (IaaS, PaaS, SaaS; siehe vorn, II.2) mietrechtliche, auftrags- oder auch werkvertragsrechtliche Komponenten enthalten kann, wobei die Qualifikation aufgrund der vielfältigen Erscheinungsformen im Einzelfall vorzunehmen ist[205].

Hauptleistungspflichten in einem Cloud-Vertrag sind die Bereitstellung der vereinbarten IT-Dienste (Services) über ein Netzwerk gegen Entgelt. Weitere Punkte, die praxisgemäss geregelt werden, sind die Art der Nutzung, die Zusammenarbeit mit dem Cloud-Provider über die Benutzerschnittstelle, Lizenzierungsfragen, Nutzungsbeschränkungen, Datensicherheit und Datenschutz sowie Dauer und Beendigung des Vertrags[206].

b) Bearbeiten wie Auftraggeber

Die Anbieter von Cloud-Diensten dürfen die von den Anwältinnen und Anwälten an sie übermittelten Personendaten nur so bearbeiten, wie es diese als Auftraggeber selbst tun dürften (Art. 10a lit. a DSG). Sie können dabei dieselben Rechtfertigungsgründe geltend machen wie die Anwältinnen und Anwälte als deren Auftraggeber (Art. 10a Abs. 3 DSG).

Anwältinnen und Anwälte bearbeiten regelmässig Personendaten über ihre Klienten, über Vertragspartner oder Gegenparteien der Klienten sowie über Dritte. Die Bearbeitung dieser Daten ist zulässig, wenn dadurch die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt wird (Art. 12 Abs. 1 DSG). Dies ist grundsätzlich der Fall, wenn die Grundsätze der Datenbearbeitung eingehalten werden (Art. 12 Abs. 2 lit. a DSG), die Daten nicht gegen den ausdrücklichen Willen der betroffenen Person bearbeitet werden (Art. 12 Abs. 2 lit. b DSG) und Dritten keine besonders schützenswerten Da-

---

205 DE LA CRUZ, Jusletter IT 15. Mai 2013, Rn. 12 und 15; STRAUB, AJP 2014, 906.

206 Siehe GRAMIGNA, Cloud-Vertrag, *passim*.

ten oder Persönlichkeitsprofile bekannt gegeben werden (Art. 12 Abs. 2 lit. c DSG). Trifft dies nicht zu, ist die Bearbeitung der Personendaten nur zulässig, wenn ein Rechtfertigungsgrund vorliegt[207]. Ein solcher besteht entweder in der Einwilligung des Verletzten, im Vorliegen eines überwiegenden privaten oder öffentlichen Interesses oder in einer gesetzlichen Grundlage (Art. 13 Abs. 1 DSG).

Anwältinnen und Anwälte werden Daten über ihre Klienten regelmässig gestützt auf deren Einwilligung bearbeiten. Häufig werden sie sich allerdings auch auf ein überwiegendes privates Interesse stützen müssen, so namentlich um die Daten Dritter, insb. der Gegenpartei, bearbeiten zu dürfen. In hängigen Gerichtsverfahren gilt das Datenschutzrecht nicht (vgl. Art. 2 Abs. 2 lit. c DSG), weil sonst die spezialgesetzlichen Normen des Verfahrensrechts unterlaufen würden[208].

Soweit die Bearbeitung von Personendaten durch die Anwältinnen und Anwälte zulässig ist, dürfen die Daten auch von den Anbietern von Cloud-Diensten bearbeitet werden. Unzulässig wäre allerdings eine Bearbeitung zu eigenen Zwecken der Dienstleister[209]. Um sicherzustellen, dass der Cloud-Provider die Daten nicht anders bearbeitet als die Anwältinnen und Anwälte, sollte die Art der Bearbeitung der Daten durch den Cloud-Provider im Cloud-Vertrag oder in einem Annex dazu festgelegt werden[210]. Dabei kann z.B. festgehalten werden, dass die Daten – unter Vorbehalt einer besonderen Weisung – nur zur Vertragserfüllung bearbeitet werden dürfen[211].

---

207 ROSENTHAL, in: Rosenthal/Jhöri, DSG 12 N 1 f.; SHK-DSG, WERMELINGER, DSG 12 N 3.

208 Vgl. JHÖRI/ROSENTHAL, in: Rosenthal/Jhöri, DSG 2 N 29; SHK-RUDIN, DSG 2 N 26.

209 SHK-DSG, BAERISWYL, DSG 10a N 26.

210 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 71.

211 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 72.

c) Keine entgegenstehenden Geheimhaltungspflichten

Die Bearbeitung von Personendaten durch Dritte ist nicht zulässig, wenn gesetzliche oder vertragliche Geheimhaltungspflichten eine solche verbieten (Art. 10a Abs. 1 lit. b DSG). Diese Verpflichtungen zur Vertraulichkeit gehen der Regelung der Auftragsdatenbearbeitung vor[212]. Unzulässig ist eine Auftragsdatenbearbeitung aber nicht schon allein aufgrund des Bestehens einer Geheimhaltungspflicht, sondern nur, wenn die gesetzlichen oder vertraglichen Vorgaben nicht eingehalten werden[213]. Die Zulässigkeit der Auftragsdatenbearbeitung bei Bestehen von Geheimhaltungspflichten hängt damit von der Zulässigkeit der Offenbarung nach den anwendbaren Geheimhaltungsbestimmungen ab[214]. Wie vorstehend aufgezeigt wurde[215], liegt bei der Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte kein Verstoss gegen gesetzliche Geheimhaltungspflichten vor. Die Nutzung von Cloud-Diensten kann aber gegen vertragliche Geheimhaltungspflichten verstossen, wenn solche bestehen sollten.

d) Gewährleistungs- und Überwachungspflichten, insb. Datensicherheit

Bei der Auftragsdatenbearbeitung bleibt der Auftraggeber für die Einhaltung der Vorgaben des Datenschutzrechts verantwortlich[216]. Art. 10a DSG stellt klar, dass der Auftraggeber sicherzustellen hat, dass der Beauftrage die Daten nur so bearbeitet, wie der Auftraggeber sie bearbeiten darf[217]. Zudem muss insb. die Datensicherheit gewähr-

---

212 BBl 1988 II 464; ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 101; SHK-DSG, BAERISWYL, DSG 10a N 29.

213 SHK-DSG, BAERISWYL, DSG 10a N 29; gl.M.: WOHLERS, digma 2016, 115.

214 BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 13; SHK-DSG, BAERISWYL, DSG 10a N 35 f.; gl. M.: WOHLERS, digma 2016, 115.

215 Siehe vorn, III.

216 GRAMIGNA, Cloud-Vertrag, Rn. 30; SHK-DSG, BAERISWYL, DSG 10a N 2; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 11; SURY/GOGNIAT, AwR 2015, 204.

217 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 46; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 11.

leistet werden (Art. 10a Abs. 2 DSG). Da der Auftraggeber in rechtlicher Hinsicht für die Einhaltung des Datenschutzrechts verantwortlich bleibt, obwohl die technische Verantwortung insb. bei SaaS-Dienstmodellen beim Cloud-Provider liegt (siehe vorn, II.3), müssen weitere Punkte bei der Auftragsvergabe geregelt werden[218]. In Analogie zu Art. 55 OR treffen den Auftraggeber die drei curae, also die *cura in eligendo, instruendo und custodiendo*[219]. Wie er diesen Pflichten nachkommen soll, wird allerdings weder durch das DSG noch durch die VDSG geregelt.

Wer Personendaten bearbeitet, muss diese durch angemessene technische und organisatorische Massnahmen vor unbefugten Datenbearbeitungen schützen (Art. 7 DSG). Die VDSG konkretisiert diese Zielsetzungen in Art. 8 Abs. 1 dahingehend, dass der Datenbearbeiter für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten sorgen muss. Er muss dabei sicherstellen, dass Personendaten intern gesetzeskonform bearbeitet werden und auch Dritte die Personendaten nicht missbrauchen können[220].

Die erforderlichen Massnahmen beurteilen sich nach einem relativen Massstab. Zu beachten sind dabei das Risiko einer Persönlichkeitsverletzung bei der betroffenen Person, der Zweck der Datenbearbeitung, die Art der bearbeiteten Daten und der Umfang der Datenbearbei-

---

218 Eine Liste möglicher vertraglicher Vorkehrungen wurde durch den Rat der Europäischen Anwaltschaften publiziert: CCBE Guidelines on the use of cloud computing services by lawyers, Brüssel, 7. September 2012, <www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf>, 8; siehe auch: privatim, Konferenz der schweizerischen Datenschutzbeauftragten, Merkblatt «Cloud-spezifische Risiken und Massnahmen», <www.privatim.ch/wpcontent/uploads/2019/02/privatim_Merkblatt_Cloud_v1.0_20190206.pdf>, 3 ff.; SURY/GOGNIAT, AwR 2015, *passim*; GRAMIGNA, Datenschutz und Outsourcing, *passim*.

219 BBl 1988 II 413, 463 f.

220 SHK-DSG, BAERISWYL DSG 7 N 13.

tung[221]. Absolute Sicherheit wird nicht vorausgesetzt[222]. Erforderlich ist vielmehr eine Risikoanalyse anhand verschiedener Kriterien, namentlich Zweck, Art und Umfang der Bearbeitung, Risiken für betroffene Personen und Stand der Technik (Art. 8 Abs. 2 VDSG). Der Inhaber einer Datensammlung, also eines Bestandes von Personendaten, der nach betroffenen Personen erschliessbar ist (Art. 3 lit. g DSG), ist gemäss Art. 9 VDSG verpflichtet, besondere Kontrollmassnahmen zu treffen: Unbefugte Personen dürfen keinen Zugang zu Einrichtungen oder automatisierten Datenverarbeitungssystemen haben, in denen Personendaten bearbeitet werden, und auch keine Datenträger lesen, kopieren, verändern oder entfernen. Bei der Bekanntgabe von Personendaten ist ebenso unberechtigtes Lesen, Kopieren, Verändern oder Löschen der Daten zu verhindern. Berechtigte Personen dürfen zudem nur zu denjenigen Daten Zugang haben, die sie zur Aufgabenerfüllung benötigen. Aufgrund letztgenannter Verpflichtungen muss überprüfbar sein, wer welche Manipulationen an den Daten vorgenommen hat, die in einem automatisierten System gespeichert sind.

Die erforderlichen technischen Massnahmen hängen direkt mit dem Informationssystem zusammen[223] und umfassen bspw. die Verschlüsselung (bei Speicherung und Übertragung), Zugriffsverwaltung, Protokollierung und Back-ups[224]. Weder das DSG noch die VDSG schrei-

---

221 SHK-DSG, BAERISWYL, DSG 7 N 23; EPINEY, § 9 N 53; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 9; BUNDESAMT FÜR JUSTIZ, Kommentar VDSG, Abs. 6.1.1.

222 SHK-DSG, BAERISWYL DSG 7 N 22; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 9; EPINEY, § 9 N 53; BUNDESAMT FÜR JUSTIZ, Kommentar VDSG, Abs. 6.1.1.

223 EDÖB, Leitfaden Massnahmen des Datenschutzes, 5; BSK-DSD/BGÖ, STAMM-PFISTER, DSG 7 N 11; SHK-DSG, BAERISWYL, DSG 7 N 19.

224 SHK-DSG, BAERISWYL DSG 7 N 19; EPINEY, § 9 N 56; ROSENTHAL, in: Rosenthal/Jhöri, DSG 7 N 8; EDÖB, Leitfaden Massnahmen des Datenschutzes, August 2015, *passim*; Es wird empfohlen, Backups auf einer Festplatte im Eigentum der Kanzlei zu machen, da so auch eine Herausgabe im Konkurs gewährleistet ist (SURY/GOGNIAT, AwR 2015, 204 f. sowie CHAPPUIS/ALBERINI, AwR 2017, 341, die fordern, dass sich die Festplatte in der Schweiz befinden soll. Siehe zu letzterem, IV.3.1e) sowie III.1.2b)v).

ben dabei spezifische technische Lösungen vor[225]. Als Orientierungshilfe wird teilweise auf internationale Standards verwiesen (z.B. ISO 27001, ISO 27002, COBIT, BSI 100-1, BSI 100-2, BSI 100-3 und BSI 100-4)[226]. Es ist nicht erforderlich, die konkret getroffenen technischen und organisatorischen Massnahmen offen zu legen, da dies die Sicherheitsziele beeinträchtigen würde[227].

Im E-DSG wird die bestehende Regelung zur Datensicherheit weitgehend übernommen. Im Vergleich zum VE-DSG findet sich die Ergänzung, dass die ergriffenen Massnahmen es ermöglichen müssen, Verletzungen der Datensicherheit zu vermeiden (Art. 7 Abs. 2 E-DSG). Es dürfte sich hierbei um die Regelung einer Selbstverständlichkeit handeln. Neu ist hingegen das Konzept des Datenschutzes durch Technik («*Privacy by Design*»), nach welchem der Verantwortliche die Datenbearbeitung schon in der Planung technisch und organisatorisch so auszugestalten hat, dass die Datenschutzvorschriften, insb. die Grundsätze der Datenbearbeitung, eingehalten werden (Art. 6 E-DSG). Diese Pflicht trifft aber gemäss Gesetzeswortlaut nicht den Auftragsdatenbearbeiter[228].

Da die wenigsten Anwältinnen und Anwälte die IT-Sicherheit des Cloud-Providers selber beurteilen können, kann der Beizug eines unabhängigen IT-Spezialisten angezeigt sein[229]. Weiter darf auch auf eine Zertifizierung vertraut werden, etwa auf ein zertifiziertes Qualitätsmanagementsystem des Cloud-Provider nach ISO 9001 bzw. ISO 27001 oder auf eine datenschutzspezifische Zertifizierung (z.B. GoodPriv@cy, VDSZ:2014 oder ePrivacy). Der Überwachungspflicht kommt der Anwalt bzw. die Anwältin am besten nach, wenn er oder sie den Anbieter verpflichtet, einen gewissen Zertifizierungsstandard einzuhalten. Ferner kann der Cloud-Provider verpflichtet werden,

225 BUNDESAMT FÜR JUSTIZ, Kommentar VDSG, Abs. 6.1.1.
226 SHK-DSG, BAERISWYL, DSG 7 N 37; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 21.
227 Vgl. BGE 144 I 126, E. 8.3.6.
228 So schon Art. 18 VE-DSG; ROSENTHAL, Jusletter 20. Februar 2017, Rn. 11.
229 SURY/GOGNIAT, AwR 2015, 203.

dem Auftragsgeber einen allfälligen Verlust der Zertifizierung oder andere datensicherheitsrelevante Aspekte mitzuteilen. Das E-DSG sieht vor, dass der Auftragsdatenbearbeiter dem Auftraggeber Verletzungen der Datensicherheit melden muss, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen (vgl. Art. 22 Abs. 3 E-DSG); zudem wird ausdrücklich geregelt, dass der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung des Auftraggebers an einen Sub-Unternehmer übertragen darf (Art. 8 Abs. 3 E-DSG). Letzteres entspricht allerdings den schon heute üblichen Massnahmen, um die Einhaltung des Datenschutzrechts durch den Auftragsbearbeiter zu überwachen[230].

e) Auslagerung ins Ausland

i. Grenzüberschreitende Bekanntgabe

Speichert der Anbieter von Cloud-Diensten die Personendaten im Ausland, liegt nach überwiegender Lehre und nach der Rechtsprechung des Bundesgerichts eine grenzüberschreitende Bekanntgabe von Daten vor (Art. 6 DSG)[231]. Teilweise wird allerdings auch vertreten, dass es an einer grenzüberschreitenden Bekanntgabe fehle, weil es sich bei der Auftragsdatenbearbeitung nicht um eine Datenbekanntgabe im Sinn des Datenschutzrechts handle[232].

Werden Daten ins Ausland transferiert, unterstehen sie unter Umständen einem schwächeren rechtlichen Schutz oder Zugriffsrechten ausländischer Behörden. Die grenzüberschreitende Bekanntgabe von Personendaten wird deshalb in Art. 6 DSG gesondert geregelt. Art. 3

---

230 Siehe ROSENTHAL, Jusletter 27. November 2017, Rn. 53.

231 BGE 144 I 126, E. 8.3.6; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 7; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 22d; GRAMIGNA, Datenschutz und Outsourcing, Rz. 20.24; STRAUB, AJP 2014, 914; SCHWANINGER/LATTMANN, Jusletter 11. März 2013, Rn. 15.

232 SHK-DSG, BAERISWYL, DSG 10a N 43 mit Verweis auf N 6; WIDMER, digma 2014, 32.

lit. f DSG definiert die Bekanntgabe als Zugänglichmachen von Daten. Beispielhaft werden vom Gesetz die Weitergabe, das Einsichtgewähren und das Veröffentlichen von Daten genannt[233]. Erfasst ist jeder Vorgang, der es Dritten ermöglicht, vom Inhalt der Daten Kenntnis zu nehmen[234]. Der Remote-Zugriff aus dem Ausland, z.B. im Rahmen einer Fernwartung der Cloud, qualifiziert daher als grenzüberschreitende Bekanntgabe[235]. Umstritten ist dabei allerdings, ob es auf den tatsächlich möglichen oder auf den vertraglich vereinbarten Zugriff ankommen soll[236]. Da Art. 6 DSG Gefährdungen der Persönlichkeit der betroffenen Person verhindern will (Abs. 1), drängt sich eine risikobasierte Interpretation auf: Ein vertraglicher Ausschluss der Bekanntgabe ins Ausland erscheint daher grundsätzlich als genügend, wenn nicht angenommen werden muss, dass sich der Cloud-Provider nicht an diese Vorgabe halten wird[237].

ii. Voraussetzungen

Nach Art. 6 Abs. 1 DSG ist eine grenzüberschreitende Bekanntgabe nur zulässig, wenn die Persönlichkeit der betroffenen Person nicht schwerwiegend gefährdet wird. Eine solche Gefährdungslage liegt gemäss Gesetz vor, wenn im Empfängerland keine hinreichende Datenschutzgesetzgebung existiert. Der EDÖB veröffentlicht gemäss Art. 7 VDSG hierzu eine unverbindliche Liste der Staaten, die seiner

233 SHK-DSG, RUDIN, DSG 3 N 41.

234 BSK-DSG/BGÖ, BLECHTA, DSG 3 N 77; SHK-DSG, RUDIN, DSG 3 N 41; PASSADELIS, Rz. 6.41.

235 STRAUB, AJP 2014, 914; vgl. GRAMIGNA, Datenschutz und Outsourcing, Rz. 20.23; FISCHER/BORNHAUSER, GesKR 2016, 434 f.

236 Für den vertraglich vereinbarten Zugriff: SCHWANINGER/LATTMANN, Jusletter 11. März 2013, Rn. 19; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 9; ähnlich: STRAUB, AJP 2014, 914; THALMANN, sic! 2007, 339; auf die tatsächlichen Zugriffsmöglichkeiten abstellend: BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 22d.

237 ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 9; STRAUB, AJP 2014, 914 Fn. 82. Das Bundesgericht lässt im Zusammenhang mit der Datensicherheit ebenso eine rechtliche Absicherung genügen, da nie ausgeschlossen werden könne, dass sich Einzelpersonen rechtswidrig verhalten (vgl. BGE 144 I 126, E. 8.3.6).

Ansicht nach einen angemessenen Datenschutz gewährleisten[238]. Für diese Staaten besteht eine widerlegbare Vermutung, dass sie ein angemessenes Datenschutzniveau gewährleisten[239]. Verlässt sich der Bearbeiter im guten Glauben auf die Liste des EDÖB, ist eine Bekanntgabe zulässig[240].

Eine Bekanntgabe von Daten in Staaten, die nicht auf der Liste des EDÖB stehen[241], ist dennoch möglich, wenn einer der Tatbestände von Art. 6 Abs. 2 DSG erfüllt ist. Vorliegend relevant sind hinreichende Garantien (lit. a), die Einwilligung der betroffenen Person (lit. b), die Bearbeitung von Personendaten des Vertragspartners im unmittelbaren Zusammenhang mit einem Vertrag (lit. c) und die Bekanntgabe innerhalb oder zwischen juristischen Personen unter einheitlicher Leitung (lit. g).

Während für Daten des Klienten eine Einwilligung eingeholt werden kann, ist dies für Daten von Gegenparteien und anderen Dritten schon aus Gründen des Geheimnisschutzes keine taugliche Lösung. Eine Anwaltskanzlei sollte sich von einem ausländischen Cloud-Provider daher hinreichende Garantien bezüglich der Einhaltung des

238 EDÖB, Stand des Datenschutzes weltweit, Stand 12. Januar 2017, <https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf.>, zuletzt besucht 12. Februar 2019.

239 OGer Zürich, Urteil vom 3. März 2015, LF140075, E. 3.2; PASSADELIS, Rz. 6.44.

240 BSK-DSG/BGÖ, MAURER-LAMBROU/STEINER, DSG 6 N 18b; EDÖB, Datenübermittlung ins Ausland, 4.

241 Die EU-Staaten haben alle das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (sog. Konvention-108; SR. 0.235.1) unterschrieben, das den Vertragsstaaten die Einschränkung des freien Verkehrs personenbezogener Daten untereinander grundsätzlich verbietet (Art. 12 Konvention-108). Die USA sind der Konvention-108 nicht beigetreten und bieten gemäss Ansicht des EDÖB keine Gewähr für ein angemessenes Datenschutzniveau.

Datenschutzes geben lassen oder einen Schweizer Anbieter wählen. Der EDÖB hat hierzu Musterverträge erarbeitet[242].

f) Exkurs: Bekanntgabe in die USA

i. Privacy-Shield Zertifizierung als hinreichende Garantie

Mit Blick auf die Marktanteile US-amerikanischer Cloud-Provider ist die Frage der Bekanntgabe von Personendaten in die USA von besonderer Bedeutung. Anders als die Mitgliedstaaten der EU bieten die USA nach Ansicht des EDÖB grundsätzlich keine Gewähr für ein angemessenes Datenschutzniveau[243]. Seit dem 12. April 2017 können sich US-Unternehmen deshalb für das Swiss-US Privacy Shield zertifizieren, welches das US-Swiss Safe-Harbor Abkommen von 2008 ersetzt[244]. Damit verpflichten sie sich, die im Privacy Shield vorgesehenen Grundsätze der Bearbeitung von Personendaten einzuhalten. Die Erklärung der US-Unternehmen, diesen Verhaltenskodex zu befolgen, ist eine hinreichende Garantie im Sinn von Art. 6 Abs. 2 lit. a DSG, welche den Datentransfer in die USA ermöglicht[245]. Mit dem Privacy Shield wird aber (wie schon mit dem Safe Harbor Framework) nicht

---

242 EDÖB, Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html>. Der EDÖB ist über die bei der Bekanntgabe ins Ausland abgegebenen Garantien zu informieren (Art. 6 Abs. 3 DSG; GRAMIGNA, Datenschutz und Outsourcing, Rz. 20.26). Bei der Bekanntgabe gestützt auf Musterverträge des EDÖB ist es ausreichend, den EDÖB in allgemeiner Weise hierüber zu orientieren (Art. 6 Abs. 3 VDSG; SHK-DSG, BAERISWYL/BLONSKI, DSG 6 N 51).

243 Siehe EDÖB, Datenübermittlung ins Ausland, 3; EDÖB, Staatenliste, 11; siehe auch PASSADELIS, Rz. 6.49; GRAMIGNA, Datenschutz und Outsourcing, Rz. 20.26.

244 Siehe hierzu die Liste des US Department of Commerce: <https://www.privacyshield.gov/list>, zuletzt besucht am 7. Februar 2019.

245 BBl 2003 2101, 2129; BSK-DSG/BGÖ, MAURER-LAMBROU/SCHÄFER, DSG 6 N 25; SHK-DSG, BAERISWYL/BLONSKI, DSG 6 N 20; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 49.

die Angemessenheit des Datenschutzniveaus in den USA festgestellt[246].

Ob eine hinreichende Garantie im Sinn von Art. 6 Abs. 2 lit a DSG vorliegt, ist nach Art. 31 Abs. 1 lit. e DSG vom EDÖB zu beurteilen. Dieser hat dies bis anhin bejaht. Fraglich erscheint allerdings, ob die Garantie künftig wegen der Zugriffsrechte von US-Behörden als unzureichend qualifiziert werden könnte. Dieses Risiko kann nicht ausgeschlossen werden, zumal gerade diese Zugriffsrechte ein massgeblicher Grund waren, weshalb der EuGH die Entscheidung 2000/520/EG der EU-Kommission vom 26. Juli 2000[247] über die Angemessenheit des Schutzes durch das Safe Harbour Framework aufgehoben hat[248]. Im Vordergrund stand dabei, dass die Kommission ein angemessenes Datenschutzniveau für unter dem Safe-Harbor Abkommen zertifizierte Unternehmen bejaht hatte, ohne die Rechtslage in den USA hinreichend zu prüfen[249]. Entscheidend war unter anderem, dass US-Gesetze dem Safe-Harbor Framework vorbehalten wurden, was den Zugriff von US-Behörden auf in die USA übermittelte Personendaten ermöglicht hat[250]. Dem Swiss-US Privacy Shield ging hingegen eine mehrjährige Konsultation voraus, in der die USA dem EDÖB Aufschluss über die rechtlichen Rahmenbedingungen

246 Siehe aber ROSENTHAL/KAISER, Jusletter 2. November 2015, Rn. 3; PASSADELIS, Rz. 6.46; FISCHER/BORNHAUSER, GesKR 2016, 436; SIDLER/VASELLA, sic! 2016, 193, gemäss denen ein angemessenes Datenschutzniveau im Sinn von Art. 6 Abs. 1 DSG hergestellt wird.

247 Entscheidung 2000/520/EG: 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, Abl L 215, 25.08.2000, 7-47.

248 EuGH, Urteil vom 6. Oktober 2015, C-362/14, *Schrems*.

249 EuGH, Urteil vom 6. Oktober 2015, C-362/14, *Schrems*, Rn. 83. Siehe auch RÜPKE/VON LEWINSKI/ECKHARDT, 270.

250 EuGH, Urteil vom 6. Oktober 2015, C-362/14, *Schrems*, Rn. 87.

behördlicher Zugriffsrechte gaben[251]. Solange der EDÖB – durchaus zu Recht – auch weiterhin davon ausgeht, dass der Swiss-US Privacy Shield als hinreichende Garantie anzusehen ist, stellt die theoretische Möglichkeit eines Zugriffs von US-Behörden die Zulässigkeit der grenzüberschreitenden Bekanntgabe deshalb wohl erst in Frage, wenn konkrete Anzeichen bestehen, dass ein solcher Zugriff systematisch oder zumindest im konkreten Einzelfall erfolgt[252].

Derzeit ist allerdings ein Verfahren vor dem EuGH hängig, welches die Zulässigkeit des Datentransfers in die USA gestützt auf hinreichende Garantien, insb. Standardvertragsklauseln, betrifft[253]. Dieses Verfahren könnte offene Fragen im Zusammenhang mit dem Datentransfer in die USA klären und dürfte – wie schon beim Safe Harbour Framework – einen Einfluss auf die Beurteilung des Swiss-US Privacy Shield durch den EDÖB haben.

ii. Hinreichende Garantien und behördliche Zugriffsrechte (Cloud Act)

Die Beurteilung des Swiss-US Privacy Shield könnte zudem durch den im März 2018 vom US-Kongress erlassenen Cloud Act[254] in Frage gestellt werden. Dieser Erlass ist eine Reaktion auf das Urteil in Sachen Microsoft v. United States, *829 F.3d 197 (2d Cir. 2016)*, mit dem der Court of Appeal for the Second Circuit entschieden hat, dass das Federal Bureau of Investigation (FBI) Microsoft gestützt auf den 1986 Stored Communications Act (SCA) nicht zur Herausgabe von Daten verpflichten könne, wenn diese auf einem Server in Irland ge-

251 Siehe die Dokumentation des Konsultationsprozesses: EDÖB, Datenübermittlung in die USA, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html>, zuletzt besucht am 26. Oktober 2018.

252 Siehe STRAUB, AJP 2014, 914 Fn. 82; MÉTILLE, medialex 2013, 63, gemäss dem sich Garantien nach Art. 6 Abs. 2 DSG nicht auf behördliche Zugriffsrechte erstrecken können; a.M. WAGNER/ZWIRNER, 172.

253 EuGH, C-311/18, *Facebook Ireland/Schrems*, noch nicht entschieden.

254 Clarifying Lawful Overseas Use of Data Act.

speichert sind[255]. Der Cloud Act regelt die territoriale Reichweite der Anordnungen («*warrants*») von US-Behörden, die sich auf im Ausland gespeicherte Daten beziehen und den Zugriff von ausländischen Behörden auf in den USA gespeicherte Kommunikationsdaten[256].

Auf der Grundlage des Cloud Act können US-Behörden auf im Ausland gespeicherte Daten zugreifen, wenn sich diese im Besitz, im Gewahrsam oder unter der Kontrolle eines US-amerikanischen Cloud-Providers befinden[257]. Der Cloud-Provider kann eine Herausgabeanordnung allerdings unter bestimmten Voraussetzungen anfechten, namentlich wenn sich diese auf einen Kunden bezieht, der weder US-Bürger ist noch in den USA wohnt und wenn die Gefahr besteht, dass ein Zugriff auf die Daten die Gesetze eines Landes verletzen würde, mit welchem die USA ein Abkommen über gegenseitige Zugriffsrechte auf Daten abgeschlossen hat[258]. Sind diese Voraussetzungen erfüllt, kann der *warrant* gerichtlich aufgehoben werden, wenn dies aufgrund einer umfassenden Interessenabwägung als angemessen erscheint[259]. Weitere Anfechtungsmöglichkeiten, insb. Rechtsmittel der von der Anordnung betroffenen Person, fehlen im Cloud Act ebenso wie Bestimmungen zum Schutz des anwaltlichen Berufsgeheimnisses[260]. Schweizerische Berufsgeheimnisse und die Vorgaben des DSG werden in diesem Verfahren nur berücksichtigt, wenn die Schweiz und die USA ein Abkommen über gegenseitige Zugriffsrechte auf Daten

255 130 Harv. L. Rev. (2016) 769 ff.; DASKAL, 71 Stan. L. Rev. Online, 9; STAIGER, 441 f.; VLCEK, 174.

256 DASKAL, 71 Stan. L. Rev. Online, 9; CORDING/GÖTZINGER, CR 2018, 636.

257 GAUSLING, MMR 2018, 579; CORDING/GÖTZINGER, CR 2018, 637.

258 18 U.S.C. § 2703(h)(2)(A–B). CORDING/GÖTZINGER, CR 2018, 637.

259 18 U.S.C. § 2703(h)(2)(B)(ii): «*based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed*»; GALBRAITH, AJIL 2018, 489; CORDING/GÖTZINGER, CR 2018, 637. Die Faktoren die in dieser Interessenabwägung («*comity analysis*») zu berücksichtigen sind, werden von 18 U.S.C. § 2703(h)(3) vorgegeben.

260 Zu Letzterem CORDING/GÖTZINGER, CR 2018, 640.

abschliessen[261]. Dieser Paradigmenwechsel umgeht das bestehende System der Rechtshilfe bewusst[262].

Wie eingangs erwähnt, könnte der Erlass des Cloud Act dazu führen, dass der EDÖB seine Einschätzung zur Angemessenheit des Datenschutzes bei US-Unternehmen ändert. Solange er aber davon ausgeht, dass beim Vorliegen einer Privacy-Shield Zertifizierung weiterhin ein angemessener Schutz besteht, ist eine Bekanntgabe von Daten in die USA vermutungsweise auch künftig zulässig. Eine risikobasierte Prüfung im Einzelfall drängt sich nur unter den für das Berufsgeheimnis relevanten Gesichtspunkten bei besonders sensiblen Daten auf[263].

3.2 Nach der DSGVO

Nach der DSGVO dürfen Personendaten nur verarbeitet werden, wenn die Grundsätze der Verarbeitung eingehalten werden (Art. 5 DSGVO) und eine der gesetzlich vorgesehenen Bedingungen für die Rechtmässigkeit der Datenverarbeitung vorliegt (Art. 6 DSGVO). Im Vordergrund stehen auch hier die Einwilligung der betroffenen Person (Art. 6 Abs. 1 Bst. a DSGVO), die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Bst. f DSGVO) und die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Bst. c DSGVO).

---

261 Daher wird gefordert, die Schweiz solle diesbezüglich Verhandlungen mit den USA aufnehmen (siehe MARKUS STÄDELI, US-Behörden können neu die Herausgabe von Daten auf ausländischen Servern verlangen, NZZ am Sonntag, 15 Dezember 2018, <https://nzzas.nzz.ch/wirtschaft/cloud-act-us-behoerden-herausgabe-von-daten-ld.1445117>, zuletzt besucht am 17. Dezember 2018).

262 DASKAL, 71 Stan. L. Rev. Online, 13. Zum bestehenden Rechtshilfesystem siehe Staatsvertrag vom 25. Mai 1973 zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (mit Briefwechseln), (RVUS), SR 0.351.933.6.

263 Siehe vorn III.1.2b)v.

a) Privilegierung der Auftragsdatenverarbeitung

Die Rechtslage für die Auslagerung einer Datenverarbeitung nach Art. 28 DSGVO entspricht in den Grundzügen derjenigen nach dem DSG. Namentlich gilt der Auftragsdatenverarbeiter nicht als Dritter, womit auch die DSGVO die Auftragsdatenverarbeitung privilegiert[264]. Für den Beizug eines Auftragsdatenverarbeiters muss deshalb nach überwiegender Auffassung keine gesonderte Bedingung für die Rechtmässigkeit (Art. 6 DSGVO) vorliegen[265]. Hinzuweisen ist allerdings auf eine in der deutschen Lehre vertretene Mindermeinung, nach welcher der Beizug eines Auftragsdatenverarbeiters nicht privilegiert werde, sondern eine Verarbeitung sei, für die eine separate Bedingung für die Rechtmässigkeit vorliegen müsse[266].

Voraussetzung für die Privilegierung der Auftragsdatenverarbeitung ist, dass der entsprechende Auftrag den von Art. 28 DSGVO verlangten Inhalt aufweist[267]. Die DSGVO gibt den Vertragsinhalt dabei weitgehend vor. Im Unterschied zum DSG lässt die DSGVO dem Verantwortlichen damit wenig Freiraum, wie er seine Pflichten bei der Auftragsdatenverarbeitung einhält.

Der Auftraggeber bleibt, wie im DSG, auch nach der DSGVO für die Einhaltung der Vorgaben des Datenschutzrechts verantwortlich[268].

---

264 PLATH, in: Plath, DSGVO 28 N 3.

265 ECKHARDT, CCZ 2017, 113; SCHMIDT/FREUND, ZD 2017, 16; im Ergebnis gleich: BERTERMANN, in: Ehmann/Selmayr, DSGVO 28 N 4 f.

266 So z.B. INGOLD, in: Sydow, DSGVO 28 N 31, der dann aber den Rechtfertigungsgrund «akzessorisch im Erlaubnisgrund der zugrunde liegenden Verarbeitung» ausmachen will, was im Endeffekt doch auf eine Privilegierung hinausläuft; siehe zu dieser Kontroverse SCHMIDT/FREUND, ZD 2017, 15.

267 ECKHARDT, CCZ 2017, 113.

268 SHK-DSG, BAERISWYL, DSG 10a N 2; BERTERMANN, in: Ehmann/Selmayr, DSGVO 28 N 11.

b) Informationspflichten

Im Unterschied zum DSG ist der Auftragsdatenverarbeiter ein Empfänger im Sinn von Art. 4 Nr. 9 DSGVO, wenn ihm Daten offengelegt werden. Dies ist im Hinblick auf die Informationspflichten von Bedeutung[269].

Werden personenbezogene Daten bei der betroffenen Person erhoben, muss der Verantwortliche ihr zum Zeitpunkt der Erhebung die Empfänger oder Kategorien von Empfängern mitteilen (Art. 13 Abs. 1 Bst. e DSGVO). Dasselbe gilt, wenn die Daten nicht bei der betroffenen Person erhoben werden (Art. 14 Abs. 1 Bst. e DSGVO). Immerhin gilt im letztgenannten Fall, dass keine Informationspflicht besteht, wenn die Daten gemäss dem Recht der Mitgliedstaaten einem Berufsgeheimnis unterstehen (Art. 14 Abs. 5 Bst. d DSGVO). Die Informationspflichten bei der Erhebung der Daten bei der betroffenen Person können gemäss Art. 23 DSGVO nach dem Recht der Mitgliedstaaten eingeschränkt werden[270].

Diese Informationspflichten sind entgegen der missverständlichen deutschen Sprachfassung keine aktiven Mitteilungspflichten, zumal die englische («*provide*»), französische («*fournir*») und italienische («*fornisce*») Fassung zeigen, dass ein blosses «Bereitstellen» oder «Mitliefern» genügt. Entsprechend muss die betroffene Person auf die Informationen zugreifen können, nicht jedoch aktiv informiert werden[271]. Entsprechende Informationen auf der Internetseite der An-

---

269 SCHREIBER, in: Plath, DSGVO 4 N 31; Im DSG muss nicht über eine Auftragsdatenbearbeitung informiert werden (SHK-DSG, BAERISWYL, DSG 10a N 13). Art. 17 Abs. 2 lit. e E-DSG schreibt eine Information über die Empfänger der Personendaten vor. Das E-DSG definiert Empfänger zwar nicht, da es aber eine Annäherung an die DSGVO bezweckt (BBl 2017 6941, 6970), wäre es angezeigt, den Auftragsdatenbearbeiter ebenfalls als Empfänger zu verstehen.

270 KAMLAH, in: Plath, DSGVO 14 N 33.

271 LAUE/NINK/KREMER, § 3 N 17; siehe auch: KAMLAH, in: Plath, DSGVO 12 N 4 und DSGVO 13 N 5.

waltskanzlei zugänglich zu machen, ist deshalb ausreichend[272]. Dabei sollte nur die Kategorie von Empfängern, d.h. eine verständliche Branchenbezeichnung, genannt werden, weil eine namentliche Nennung des Cloud-Providers der Datensicherheit abträglich wäre, zumal sie gezielte Attacken auf die Daten erleichtern würde.

c) Auslagerung ins Ausland

Datenverarbeitungen dürfen nach der DSGVO in ein Drittland ausgelagert werden. Die EWR-Staaten Island, Liechtenstein und Norwegen gelten dabei aufgrund der Übernahme der DSGVO ins EWR-Abkommen nicht als Drittländer[273]. Auch in der DSGVO ist die Bekanntgabe von Personendaten ins Ausland nicht im Kontext der Auftragsdatenverarbeitung, sondern eigens im Kapitel V (Übermittlung personenbezogener Daten an Drittländer, Art. 44 ff. DSGVO) geregelt[274]. Die Übermittlung personenbezogener Daten in Drittländer ist grundsätzlich nur zulässig, wenn die EU-Kommission beschlossen hat, dass das betreffende Drittland ein angemessenes Schutzniveau bietet (Art. 45 DSGVO)[275], der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien, wie z.B. Standardvertragsklauseln oder Binding Corporate Rules, vorgesehen hat (Art. 47 DSGVO) oder eine Einzelfal-

---

272 Solche Hinweise finden sich auch auf den Webseiten europäischer Kanzleien: Siehe z.B. Linklaters, Global Privacy Notice, No. 18, Version Mai 2018 <https://www.linklaters.com/en/legal-notices/privacy-notice>; Hengeler Mueller, Allgemeine Datenschutzbestimmungen, No. IV, <https://www.hengeler.com/de/service/datenschutz/allgemeine-datenschutzbestimmungen/>; Granrut société d'avocats, Protection des données <https://www.granrut.com/-protection-des-donnees-.html>, wobei keine der erwähnten Kanzleien die Empfänger namentlich nennt.

273 Decision of the EEA Joint Committee, No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37; siehe ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 10. Die Entscheidung des EWR-Ausschusses wurde auf den 20. Juli 2018 in Kraft gesetzt.

274 ECKHARDT, CCZ 2017, 116; ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 5; SCHRÖDER, in Kühling/Buchner, DSGVO 45 N 48.

275 ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 3.

lausnahme vorliegt. Letztere kann namentlich die Einwilligung der betroffenen Person (Art. 49 Abs. 1 Bst. a DSGVO), die Bearbeitung von Personendaten des Vertragspartners im unmittelbaren Zusammenhang mit einem Vertrag (Art. 49 Abs. 1 Bst. c DSGVO) oder die Übermittlung zur Ausübung der Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 Bst. e DSGVO) sein.

Eine Bekanntgabe in ein Drittland kann aus Sicht des Schweizer Verantwortlichen nur vorliegen, wenn die Daten in ein Nicht-EWR Land ausgelagert werden. Die Bekanntgabe innerhalb der Schweiz ist hingegen keine Bekanntgabe in ein Drittland, weil sich die Daten bereits in einem Drittland befinden. Nach aktuellem Stand verfügen aus Sicht der EU-Kommission nebst der Schweiz auch Andorra, Argentinien, Kanada (allerdings nur hinsichtlich Organisationen, die Daten im Rahmen kommerzieller Tätigkeiten verarbeiten), die Färöer, Guernsey, Israel, die Isle of Man, Jersey, Neuseeland, Uruguay und Japan über ein angemessenes Datenschutzniveau. Bei in den USA domizilierten Unternehmen wird die Angemessenheit des Datenschutzes angenommen, wenn sie sich unter dem EU-US Privacy Shield zertifiziert haben[276]. Wird ein Cloud-Provider in einem anderen Land gewählt, sollte der Cloud-Vertrag Standardvertragsklauseln zur Auslagerung ins Ausland enthalten.

[276] European Commission, Adequacy of the protection of personal data in non-EU countries, <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>, zuletzt besucht am 7. September 2018. Es lässt sich argumentieren, dass es sich beim Privacy Shield um eine hinreichende Garantie handelt. Die EU-Kommission und die h.L. bezeichnen den Privacy Shield als Sonderfall eines Angemessenheitsbeschlusses (siehe auch KLUG, in: Gola, DSGVO 45 N 11).

V. Erkenntnisse

Die vorstehende Analyse hat gezeigt, dass Anwältinnen und Anwälte bei der Ausübung ihrer beruflichen Tätigkeit die Dienste von Cloud-Providern nutzen dürfen. Dabei sind zwei Konstellationen zu unterscheiden:

Werden die Daten durch die Anwältinnen und Anwälte vor der Übertragung an den Cloud-Provider verschlüsselt und verfügt dieser nicht über den zur Entschlüsselung erforderlichen Schlüssel, liegt keine Offenbarung von Geheimnissen im Sinn von Art. 321 StGB vor, weil der Cloud-Provider keine realistische Möglichkeit hat, von den geheimen Informationen Kenntnis zu nehmen. Da verschlüsselte Daten nicht als Personendaten zu qualifizieren sind, liegt auch keine Bearbeitung von Personendaten durch den Cloud-Provider vor. In dieser Konstellation ist die Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte deshalb straf- und datenschutzrechtlich unbedenklich.

Werden die Daten nicht durch die Anwältinnen und Anwälte, sondern durch den Cloud-Provider verschlüsselt, besteht die folgende Rechtslage:

- Der Cloud-Provider ist als Hilfsperson der Anwältinnen und Anwälte zu qualifizieren, weil dieser Teil der arbeitsteilig organisierten Funktionseinheit «Anwaltskanzlei» ist; zu dieser Funktionseinheit können auch externe Personen gehören, etwa ein externes Schreibbüro, ein externer IT-Support oder ein Cloud-Provider.
- Die Möglichkeit der Kenntnisnahme durch Hilfspersonen ist kein Offenbaren eines Geheimnisses im Sinn von Art. 321 StGB, weil die Hilfspersonen zum inneren Kreis der Organisation der Anwältinnen und Anwälte gehören und definitionsgemäss Geheimnisse zur Kenntnis nehmen können.

- Die Nutzung von Cloud-Providern durch Anwältinnen und Anwälte führt damit nicht zu einer Verletzung des Berufsgeheimnisses nach Art. 321 StGB.
- Anwältinnen und Anwälte müssen den Cloud-Provider sorgfältig auswählen und die Wahrung des Berufsgeheimnisses vertraglich absichern (Art. 13 Abs. 2 BGFA). Sie müssen vereinbaren, dass Klientendaten nur zur Vertragserfüllung verwendet werden dürfen und die Einhaltung dieser Verpflichtung in zumutbarer Weise überwachen.
- Der Cloud-Provider ist als Auftragsdatenbearbeiter der Anwältinnen und Anwälte zu qualifizieren. Die durch ihn erfolgende Datenbearbeitung ist zulässig, weil damit keine gesetzlichen Geheimhaltungspflichten verletzt werden. Werden auch die weiteren Vorgaben der Auftragsdatenbearbeitung eingehalten, kann der Cloud-Provider die Daten so bearbeiten, wie es auch den Anwältinnen und Anwälten erlaubt ist. Die Nutzung der Dienste von Cloud-Providern durch Anwältinnen und Anwälte ist damit auch datenschutzrechtlich zulässig.
- Wird ein Cloud-Provider gewählt, der seinen Sitz in einem Land ohne angemessenes Datenschutzniveau hat oder haben Techniker im Rahmen einer Fernwartung von einem Land ohne angemessenes Datenschutzniveau Zugriff auf die Daten im Klartext, sollte sich der Anwalt oder die Anwältin hinreichende Garantien bezüglich der Einhaltung der Vorgaben des anwendbaren Datenschutzrechts geben lassen. Dies ist insb. für die Zusammenarbeit mit Cloud-Providern mit Sitz ausserhalb des EWR erforderlich.

Auch wenn die Nutzung von Cloud-Providern durch Anwältinnen und Anwälte straf- und datenschutzrechtlich zulässig ist, dürfte es sich im Sinn einer zusätzlichen Absicherung empfehlen, in Mandatsverträgen und Vollmachten einen Hinweis auf die Nutzung von Cloud-Providern aufzunehmen. Ein solcher Hinweis dient nicht nur

der Transparenz, sondern kann im Streitfall auch als Nachweis der Einwilligung in die Nutzung eines Cloud-Providers dienen.