AUF DEM WEG ZUR DIGITALEN ANWALTSKANZLEI TROTZ BERUFSGEHEIMNIS UND DATENSCHUTZ

DANIEL HÜRLIMANN
Dr. iur., Rechtsanwalt, Laux Lawyers AG, Zürich,
Lektor an der Universität Freiburg

MARTIN STEIGER
Lic. iur. HSG, Anwalt und Unternehmer für Recht im digitalen Raum,
Steiger Legal AG, Zürich

Stichworte: Digitalisierung, DSG, Datenschutzrecht, Anwaltsrecht, Berufsgeheimnis

Gesetzgeber und Markt verlangen von allen Anwältinnen und Anwälten, den Weg zur digitalen Anwaltskanzlei zu beschreiten. Die Nutzung von digitalen Arbeitswerkzeugen und insbesondere Cloud-Diensten ist weniger problematisch als gemeinhin angenommen. Der vorliegende Beitrag zeigt auf, was datenschutzrechtlich, anwaltsrechtlich und strafrechtlich zulässig ist. Anhand von vier beispielhaften Onlinediensten wird aufgezeigt, was die rechtlichen Voraussetzungen in der Praxis bedeuten.

I. Einleitung

Die Digitalisierung schreitet in der Schweiz voran. Viele Anwaltskanzleien haben sich allerdings bisher darauf beschränkt, E-Mail zu verwenden und allenfalls das klobige Faxgerät zu entsorgen. Gleichzeitig setzt die wachsende, nicht anwaltlich regulierte Konkurrenz – Legal-Tech-Start-ups sowie Beratungsunternehmen und Rechtsschutzversicherungen – fast ausschliesslich auf Arbeitsmittel im digitalen Raum.[1]

Technologiefeindlichkeit ist nicht immer der Grund für die Zurückhaltung bei Anwältinnen und Anwälten. Eine wesentliche Rolle spielen das Berufsgeheimnis und der Datenschutz. Häufig ist nicht klar, ob die Nutzung von Cloud-Diensten sowie Outsourcing überhaupt datenschutzrechtlich, anwaltsrechtlich oder strafrechtlich zulässig ist. Wer sich nicht eingehend mit der Thematik befassen will, verzichtet daher tendenziell auf die Nutzung solcher Arbeitsmittel.

Aufgrund der COVID-19-Pandemie mussten sich viele Anwaltskanzleien in der Schweiz mit der Digitalisierung befassen, ob sie wollten oder nicht. Anwälte, die nicht allein tätig sind, benötigen für die Tätigkeit im Homeoffice digitale Arbeitsmittel und Cloud-Dienste. Beispiele dafür sind der gemeinsame Zugriff auf Akten und Dokumente sowie die Kommunikation mit Mandantinnen und Mandanten wie auch teilweise mit Behörden per Videokonferenz.[2]

Anwälte, welche die Vorteile digitaler Arbeitsmittel kennengelernt haben, werden nicht mehr darauf verzichten wollen. Viele Anwältinnen werden aus dem Homeoffice nicht mehr vollständig an einen Arbeitsplatz in einer Kanzlei zurückkehren. Selbst jene, die Sehnsucht nach papierbasiertem Arbeiten «wie früher» verspüren, werden sich der Digitalisierung stellen müssen. Rechtlicher Hauptgrund ist das neue E-Justice-Gesetz[3], das mittels Anpassungen der Prozessordnungen ein Obligatorium für die elektronische Übermittlung vorsieht.[4] Unabhängig von der Diskussion, ob dieses Obligatorium zu begrüssen ist, wird das E-Justice-Gesetz für viele Anwaltskanzleien den Anlass bieten, auch intern grossmehrheitlich auf digitale Arbeitsmittel zu wechseln.[5]

1 Vgl. auch SCHWANINGER ET AL., [https://perma.cc/7VJG-4SZW Legaltech-Trends in der Schweiz], in: Anwaltsrevue 6/7/2020, S. 247 ff.
2 Die Autoren erarbeiteten diesen Beitrag mit Google Docs.
3 Vorentwurf vom 11. 11. 2020 zu einem Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ).
4 S. dazu die im Anhang des Vorentwurfs für ein E-Justice-Gesetz enthaltenen Vorentwürfe für einen neuen Art. 47a VwVG, einen neuen Art. 38c BGG, einen neuen Art. 128c ZPO, einen neuen Art. 103c StPO, einen neuen Art. 2c ZeugSG, einen neuen Art. 8c OHG, einen neuen Art. 31c VStrR und einen neuen Art. 37c MStP (alle mit dem Titel «Obligatorische elektronische Übermittlung») sowie einen neuen Art. 37a VGG («Elektronische Übermittlung») und einen neuen Art. 8 Abs. 1 Bst. e BGFA (Zustelladresse auf der E-Justiz-Plattform als Voraussetzung für den Anwaltsregistereintrag).
5 Vgl. auch JACQUES BÜHLER/BARBARA WIDMER, Auf dem Weg zur digitalen Justiz – Ein Statusbericht, in: Anwaltsrevue 4/2021, S. 169 ff.

Dieser Weg zur digitalen Anwaltskanzlei ist – bei genauer Betrachtung – weniger problematisch als gemeinhin angenommen wird, wie dieser Beitrag zeigen soll. Das gilt nicht nur anwalts- und strafrechtlich, sondern auch unter dem geltenden und künftigen Datenschutzgesetz in der Schweiz.

II. Rechtsgrundlagen

1. Datenschutzrecht

Anwältinnen und Anwälte in der Schweiz unterliegen – wie grundsätzlich alle privaten Personen, die Personendaten bearbeiten – immer und vollständig dem schweizerischen Datenschutzrecht. Das geltende Bundesgesetz über den Datenschutz (DSG) wird voraussichtlich in der zweiten Jahreshälfte 2022 durch das vollständig revidierte DSG (revDSG) abgelöst.[6] Mit dem revDSG wird unter anderem versucht, mit neuen Strafbestimmungen einen Anreiz zur Einhaltung bestehender datenschutzrechtlicher Grundsätze und Pflichten zu schaffen. Weiter soll sichergestellt werden, dass die Europäische Kommission weiterhin zum Ergebnis gelangt, das schweizerische Recht gewährleiste einen angemessenen Datenschutz, um den freien Datenverkehr zwischen der Schweiz und Europa zu sichern.[7]

Das absehbare Inkrafttreten des revDSG ist – nach der Anwendbarkeit der europäischen Datenschutz-Grundverordnung (DSGVO) per 25. 5. 2018 – eine weitere Chance für Anwältinnen in der Schweiz, sich vertieft mit den Auswirkungen des Datenschutzrechtes auf ihre berufliche Tätigkeit zu befassen. Das Datenschutzrecht zählt zu den Compliance-Vorschriften, die jede Anwaltskanzlei einhalten muss.[8] Damals mussten schweizerische Anwälte prüfen, ob sie teilweise der DSGVO unterliegen und die DSGVO ergänzend zum DSG einhalten müssen. Die DSGVO ist für schweizerische Anwältinnen insbesondere dann teilweise anwendbar, wenn sie sich an Mandantinnen und Mandanten im Europäischen Wirtschaftsraum (EWR)[9] richten (Art. 3 Abs. 2 lit. a DSGVO, Marktortprinzip) oder wenn sie sich gegenüber Mandanten vertraglich zur Einhaltung der DSGVO verpflichten. Anwälte im Anwendungsbereich der DSGVO müssen insbesondere die Rechtmässigkeit der Verarbeitung von personenbezogenen Daten sicherstellen, da die DSGVO eine solche Verarbeitung nur ausnahmsweise erlaubt (Art. 6 DSGVO, Verbot mit Erlaubnisvorbehalt). Ausserdem vereinheitlichte und verschärfte die DSGVO für Europa unter anderem die Anforderungen an die Gewährleistung der Datensicherheit, die Dokumentations- und Informationspflichten sowie die Vorgaben für das Outsourcing der Verarbeitung (Auftragsverarbeitung). Wer im Anwendungsbereich der DSGVO die Daten von Personen im EWR in einem Drittstaat – dazu zählt die Schweiz – bearbeitet, benötigt weiter in vielen Fällen eine EU-Datenschutz-Vertretung (Art. 27 DSGVO). Datenschutz-Aufsichtsbehörden erhielten mit der DSGVO neue Kompetenzen und können beispielsweise abschreckend hohe Geldbussen verhängen (Art. 83 DSGVO).[10]

Für die Nutzung von digitalen Arbeitswerkzeugen durch Anwältinnen stehen sowohl im geltenden DSG als auch im revDSG die Bestimmungen über die Gewährleistung der Datensicherheit (Art. 7 DSG bzw. Art. 8 revDSG) und die Auftragsbearbeitung (Art. 10a DSG – als «Datenbearbeitung durch Dritte» bezeichnet – bzw. Art. 9 revDSG) im Vordergrund.

Anwälte, welche die DSGVO umgesetzt haben, werden feststellen, dass sie das revDSG in weiten Teilen bereits umgesetzt haben. Für alle Anwältinnen ist es aber empfehlenswert, sich mit den Bestimmungen des revidierten Datenschutzrechts zu befassen.[11] Anwälte, die das revDSG nicht oder nicht rechtzeitig umsetzen, riskieren bei Datenschutzverletzungen eine Untersuchung sowie Verwaltungsmassnahmen durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB, Art. 49 ff. revDSG) sowie Verfahren durch kantonale Strafverfolgungsbehörden mit persönlichen Bussen bis zu 250 000 Franken (Art. 60 ff.).[12] Immerhin besteht im schweizerischen Datenschutzrecht weiterhin kein Rechtfertigungszwang für die Bearbeitung von Personendaten, sondern die Bearbeitung ist unter Einhaltung der datenschutzrechtlichen Grundsätze erlaubt (Art. 6 revDSG, unter anderem Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Transparenz und Zweckbindung), solange sie nicht ausnahmsweise verboten ist (Erlaubnis mit Verbotsvorbehalt). Auch das gemäss DSGVO häufige Erfordernis einer Einwilligung bleibt dem schweizerischen Datenschutzrecht fremd.[13] Informationen in Datenschutzerklärungen und an anderen Stellen sollen die Personen, deren Daten bearbeitet werden, befähigen, ihre Rechte wahrzunehmen (Art. 19 ff. revDSG), insbesondere bei einer Verletzung ihrer Persönlichkeit.

Beim Übergang vom geltenden DSG zum revDSG bleibt unverändert, dass das Datenschutzrecht die Anwaltstätigkeit in allen Aspekten erfasst. Das liegt daran, dass der Geltungsbereich der «Bearbeitung von Perso-

---

6 Das Datenschutzteam der Walder Wyss AG hat unter [https://datenrecht.ch/rev-dsg/] das revDSG in lesefreundlicher Form aufbereitet und mit Auszügen aus der bundesrätlichen Botschaft ergänzt, zuletzt abgerufen am 30. 4. 2021.

7 Vgl. Bundesamt für Justiz, [https://perma.cc/39VW-EXAK Stärkung des Datenschutzes], Totalrevision des Bundesgesetzes über den Datenschutz (DSG), zuletzt abgerufen am 30. 4. 2021.

8 Vgl. auch BENOÎT CHAPPUIS/STÉPHANIE CHUFFART-FINSTERWALD, La Compliance dans les études d'avocat: Quelques sujets topiques choisis, in: Anwaltsrevue 3/2020, S. 121 ff.

9 Der Europäische Wirtschaftsraum (EWR), [https://perma.cc/48XS-NETN Europäische Wirtschaftsraum], umfasst die 27 Mitgliedstaaten der Europäischen Union (EU) sowie das Fürstentum Liechtenstein, Island und Norwegen, zuletzt abgerufen am 30. 4. 2021.

10 Vgl. ausführlich: MARTIN STEIGER, Neues EU-Datenschutz-Recht: Was gilt für Anwaltskanzleien; in: Anwaltsrevue 5/2018, S. 205 ff.

11 Vgl. ausführlich: DAVID ROSENTHAL, [https://perma.cc/J7NK-DQH9 Das neue Datenschutzgesetz], in: Jusletter, 16. 11. 2020.

12 Vgl. ausführlich: DAVID ROSENTHAL/SERAINA GUBLER, Die Strafbestimmungen des neuen DSG, in: SZW 1/2021, S. 52 ff.

13 Art. 6 Abs. 7 revDSG regelt nicht, dass in den genannten Fällen eine Einwilligung erforderlich ist, sondern stellt klar, dass eine allfällige Einwilligung – zum Beispiel als Rechtfertigungsgrund für eine ansonsten widerrechtliche Persönlichkeitsverletzung (Art. 31 Abs. 1 revDSG) – in diesen Fällen ausdrücklich erfolgen muss.

nendaten natürlicher Personen» äusserst breit gefasst ist. Personendaten sind «alle Angaben, die sich auf eine bestimmte oder *bestimmbare* natürliche Person beziehen» (Art. 5 lit. a revDSG) und Bearbeiten umfasst «*jeden* Umgang mit Personendaten, *unabhängig* von den angewandten Mitteln und Verfahren» (Art. 5 lit. d revDSG)[14]. Personendaten, die von Anwältinnen bearbeitet werden, sind ausserdem häufig «besonders schützenswert», zum Beispiel «Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie», «Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» oder «Daten über Massnahmen der sozialen Hilfe» (Art. 5 lit. c Ziff. 2, 5 u. 6 revDSG).

A) Datensicherheit

Wer Personendaten bearbeitet, muss «durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit» gewährleisten (Art. 8 Abs. 1 revDSG).[15] «Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden» (Art. 8 Abs. 2 revDSG). So müssen die Daten beispielsweise vor Verlust und unberechtigten Zugriffen geschützt werden.

Die Gewährleistung der Datensicherheit bildet faktisch den Kern der Pflichten bei der Bearbeitung von Personendaten. Es gilt, die Integrität, Verfügbarkeit und Vertraulichkeit der bearbeiteten Personendaten tatsächlich sicherzustellen und nicht bloss in der veröffentlichten Datenschutzerklärung oder in der erstellten internen Dokumentation zu behaupten. Bei einer Datenpanne wird allein die Erklärung, man habe geeignete Massnahmen getroffen, zumindest in der Kommunikation und mit Blick auf die Reputation nicht genügen. Bei besonders schützenswerten Personendaten bestehen im Übrigen auch besonders hohe Risiken für die Mandantinnen und Mandanten.

Das revDSG fordert keine absolute Datensicherheit, sondern risikobasierte Massnahmen. Gängige Massnahmen bei digitalen Arbeitswerkzeugen sind beispielsweise Datensicherung (einschliesslich möglicher Wiederherstellung der gesicherten Daten!), Zugangs- und Zugriffsbeschränkungen sowie Verschlüsselung, aber auch interne Kontrollen, Regelungen und Schulungen sowie vertragliche Absicherungen. Der Bundesrat wird auf Verordnungsebene die Mindestanforderungen an die Datensicherheit konkretisieren müssen (Art. 8 Abs. 3 revDSG). Anhaltspunkte liefern Art. 8 ff. der geltenden Verordnung zum Bundesgesetz über den Datenschutz (VDSG).[16]

Wer die bundesrätlichen Mindestanforderungen vorsätzlich nicht einhält, kann in Zukunft mit Busse bis zu 250 000 Franken bestraft werden (Art. 61 lit. c revDSG). Wer nicht riskieren möchte, die eigenen Massnahmen durch eine Übertretungsstrafbehörde beurteilen zu lassen, wird einen hohen Massstab betreffend Angemessenheit und Geeignetheit anstreben müssen.

Die Gewährleistung der digitalen Datensicherheit ist für viele Anwälte eine anspruchsvolle Aufgabe. Für Anwältinnen, welche die erforderlichen Massnahmen nicht selbst umsetzen können oder möchten, ist es häufig schwierig, die benötigte Unterstützung durch Dritte zu finden. Es gibt nur wenige Anbieterinnen und Anbieter mit der erforderlichen Kompetenz, die sich an Kleinst- und Kleinunternehmen, das heisst an die grosse Mehrheit der schweizerischen Anwaltskanzleien, richten. Anwälte gelten in der Branche als anspruchsvolle, sparsame und ungeduldige Kundschaft.

Eine Alternative zur eigenständigen Gewährleistung der Datensicherheit ist deshalb bei vielen digitalen Arbeitswerkzeugen das Outsourcing. Software wird nicht selbst betrieben und gewartet, sondern Dritte werden mit dem Betrieb und der Wartung der Software beauftragt. Datenschutzrechtlich handelt es sich um eine Auftragsbearbeitung. Ein solches Outsourcing stellt zwar – zumindest gefühlt – einen gewissen Kontrollverlust über die eigenen Daten dar, kann aber gerade bei Kleinst- und Kleinunternehmen die Datensicherheit und die tatsächliche Kontrolle über die eigenen Daten erheblich verbessern.

B) Auftragsbearbeitung

Die Beauftragung von Dritten ist im schweizerischen Datenschutzrecht ausdrücklich zulässig (Art. 8a DSG bzw. Art. 9 revDSG). Bei digitalen Arbeitswerkzeugen erfolgt das Outsourcing in erster Linie durch die Nutzung von Cloud-Diensten beziehungsweise Software-as-a-Service (SaaS)-Angeboten[17] sowie teilweise durch Remote Computing mit Fernzugriff auf herkömmliche IT-Infrastruktur, die aber von Dritten betrieben wird. Moderne Software ist häufig und zunehmend nur noch als Cloud-Dienst erhältlich, was auch den Vorteil hat, flexible Arbeitsorte für die Mitarbeiterinnen und Mitarbeiter einer Anwaltskanzlei zu ermöglichen. Wer mit einem Smartphone oder sonstigen Computer online gehen kann, kann grundsätzlich überall im Universum arbeiten. Anwaltskanzleien, die bereits SaaS-Angebote nutzten, konnten ihr Personal durch die Tätigkeit im Home- oder Remote-Office in der COVID-19-Pandemie von Anfang an wirksam schützen, ohne gleichzeitig Einbussen bei der Datensicherheit in Kauf zu nehmen.

Die Auftragsbearbeitung benötigt grundsätzlich keine Einwilligung der Personen, deren Daten bearbeitet werden. Der Auftragsbearbeiter wird – entgegen der Terminologie «Dritte» im geltenden DSG – datenschutzrechtlich der Auftraggeberin zugeordnet, sodass keine Bekanntgabe an «Dritte» erfolgt. Damit verletzen Anwältinnen, die Outsourcing nutzen, keine gesetzliche oder vertragliche Geheimhaltungspflicht, solange sie die datenschutzrechtlichen Anforderungen an die Auftragsbe-

14 Die Terminologie «Bearbeiten von Personendaten» (DSG, revDSG) und «Verarbeitung personenbezogener Daten» (DSGVO) kann im Alltag als synonym betrachtet werden.

15 Die technischen und organisatorischen Massnahmen werden üblicherweise als «TOMs» abgekürzt.

16 [https://perma.cc/NWT7-QUZA].

17 Vgl. zu diesen Begriffen die entsprechenden Wikipedia-Artikel [https://perma.cc/4Q6W-DF4H] und [https://perma.cc/KBG9-LF4M].

arbeitung erfüllen. Anwälte müssen ihre Mandanten nicht zwingend informieren, dass sie Outsourcing nutzen.

Gemäss Art. 9 Abs. 1 revDSG muss die Auftragsbearbeitung vertraglich abgesichert werden, was üblicherweise mit einem Auftragsverarbeitungsvertrag (AVV)[18] geschieht. Praxis in der Schweiz ist, dass sich solche Verträge an den detaillierten Vorgaben von Art. 28 Abs. 3 DSGVO orientieren. Damit werden unter anderem die erforderlichen Kontroll- und Weisungsrechte sowie der Beizug von weiteren Auftragsbearbeitern, das heisst von Unterauftragsbearbeitern, geregelt (Art. 9 Abs. 3 revDSG).[19]

Viele Anbieter von digitalen Arbeitswerkzeugen sitzen im Ausland. Wer solche Angebote nutzt, exportiert Personendaten und muss diesen Export absichern. Kein Datenexport liegt dann vor, wenn die Daten unter eigener Kontrolle und mit ausschliesslichem Zugriff aus der Schweiz Ende zu Ende verschlüsselt werden, was aber selten angeboten wird oder angesichts der verwendeten Art von Software gar nicht praktikabel ist.

Der Datenexport – Art. 16 ff. revDSG tragen den Titel «Bekanntgabe von Personendaten ins Ausland» – ist zulässig, wenn aus schweizerischer Sicht im Ausland ein angemessener Datenschutz gewährleistet ist. Der Bundesrat wird gemäss revDSG eine entsprechende Liste führen, während diese Aufgabe heute dem EDÖB obliegt.[20] Bei Staaten, die nicht auf dieser Liste zu finden sind, kann ein «geeigneter Datenschutz» unter anderem durch einen völkerrechtlichen Vertrag oder durch Standarddatenschutzklauseln gewährleistet werden (Art. 16 Abs. 2 lit. a u. d revDSG). Letzteres kann beispielsweise bei Auftragsbearbeitern in den USA versucht werden, nachdem die datenschutzrechtliche Absicherung in Bezug auf amerikanische Anbieter nicht mehr mit den früheren Safe-Harbor- und Privacy-Shield-Regelungen möglich ist.[21]

2. Anwaltsrecht[22]

Mit Blick auf die Frage, ob die Nutzung digitaler Arbeitswerkzeuge zulässig ist, ist das in Art. 13 BGFA verankerte Berufsgeheimnis zentral. Gemäss dieser Bestimmung unterstehen Anwältinnen und Anwälte zeitlich unbegrenzt und gegenüber jedermann dem Berufsgeheimnis gegenüber allem, was ihnen infolge ihres Berufes von ihrer Klientschaft anvertraut worden ist.

Dem Berufsgeheimnis gemäss dem BGFA als eidgenössischem Anwaltsgesetz liegt derselbe Vertraulichkeitsbegriff zugrunde wie dem strafrechtlich verankerten Berufsgeheimnis (Art. 321 StGB).[23] Wohl aus diesem Grund wird das Berufsgeheimnis gemäss Art. 13 BGFA in Abklärungen zur Zulässigkeit insbesondere der Cloud-Nutzung durch Anwältinnen teilweise gar nicht erwähnt.[24] Während eine Strafverfolgung wegen Verletzung des Berufsgeheimnisses einen Strafantrag voraussetzt, wird das im Anwaltsrecht verankerte Berufsgeheimnis durch die kantonalen Aufsichtsbehörden überwacht. Vorfälle, welche die Berufsregeln verletzen könnten, sind durch kantonale und eidgenössische Gerichts- und Verwaltungsbehörden unverzüglich der kantonalen Aufsichtsbehörde zu melden (Art. 15 BGFA).

Das Bundesgericht bestätigte mit einem im Juni 2019 gefällten Urteil die Verweigerung der Änderung eines Registereintrags durch die Genfer Anwaltsaufsichtsbehörde unter anderem wegen Nichteinhaltung des Berufsgeheimnisses.[25] Die anwaltliche Beschwerdeführerin wollte ihre Geschäftsadresse zu einer Aktiengesellschaft verlegen, deren Zweck darin besteht, als Plattform für unabhängige Anwälte zu fungieren und ihnen ein Geschäftsdomizil und/oder Dienstleistungen im Zusammenhang mit der Benutzung von Räumlichkeiten anzubieten.[26] Das Bundesgericht hielt mit Bezug auf das Berufsgeheimnis zunächst fest, dass die Aktiengesellschaft die Voraussetzungen für die Qualifikation als Hilfsperson erfülle, weil sie für die Beschwerdeführerin in Erfüllung eines Servicevertrags Leistungen erbringe, die zur Ausübung ihres Berufs beitrügen. Somit hätte die Beschwerdeführerin dafür sorgen müssen, dass die Aktiengesellschaft das Berufsgeheimnis einhält.[27]

Im konkreten Fall war dies jedoch nicht im erforderlichen Mass gewährleistet. Insbesondere fehlte es an einer schriftlichen Verpflichtung der Aktiengesellschaft, das Berufsgeheimnis zu respektieren und dafür zu sorgen, dass auch ihre Mitarbeiterinnen dieses respektieren. Aus den allgemeinen Geschäftsbedingungen ergab sich stattdessen, dass die Beschwerdeführerin akzeptierte, dass die Aktiengesellschaft ihre Haftung auf vorsätzliches oder grob fahrlässiges Verhalten beschränkte. Im Hinblick auf das Erfordernis, dass die Anwältin alle ihr zumutbaren Massnahmen ergreifen muss, um eine Verletzung des Berufsgeheimnisses zu vermeiden, sei das nicht ausreichend. Darüber hinaus wären Telefonate zum Festnetzanschluss der Aktiengesellschaft nicht durch eigene Mitarbeiterinnen, sondern durch Mitarbeiter eines von dieser beauftragten Drittunternehmens geführt worden (Subdelegation). Dritte hätten somit Zugang zu Informationen gehabt, die unter die Schweigepflicht fallen, was mit der Verpflich-

18 Die europäische Terminologie «Auftragsverarbeitungsvertrag», abgekürzt AVV, wird häufig auch in der Schweiz verwendet. Wer schon länger im Datenschutzrecht tätig ist, zeigt das gerne mit dem früher in Deutschland verwendeten Begriff «Auftragsdatenverarbeitungsvertrag» (ADV).

19 Vgl. auch SAV-Fachgruppe Digitalisierung, [https://perma.cc/NUF6-6QQF SAV-Wegleitung für IT-Outsourcing und Cloud-Computing], Juni 2019 (nur mit SAV-Login).

20 EDÖB, [https://perma.cc/9R3R-3C3P Übermittlung ins Ausland], zuletzt abgerufen am 30. 4. 2021.

21 Vgl. MARTIN STEIGER, [https://perma.cc/684F-2DVN Nach dem Ende von Privacy Shield: Wie können amerikanische Internet-Dienste weiterhin genutzt werden?], Cyon, 13. 10. 2020.

22 Vgl. u. a. ausführlich: CHRISTIAN SCHWARZENEGGER ET AL., [https://perma.cc/3M29-BTFB Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte], Zürich 2019 (zit. Gutachten) mit [https://perma.cc/C7ZF-PFMC Zusammenfassung], in: Anwaltsrevue 1/2019, S. 25 ff.

23 HANS NATER ET AL. (Hrsg.), Kommentar zum Anwaltsgesetz, Zürich 2011, Art. 13 N 16.

24 CHRISTIAN SCHWARZENEGGER ET AL., in: Anwaltsrevue 1/2019, S. 25 ff.

25 BGE 145 II 229 E. 9.

26 BGE 145 II 229 Sv. A.

27 BGE 145 II 229 E. 7.5.

tung zur Einhaltung des Berufsgeheimnisses nicht vereinbar sei.[28]

Die Arbeitsumgebung, in die sich die beschwerdeführende Anwältin begeben wollte, hätte das Berufsgeheimnis nicht garantiert. Somit war es gemäss Bundesgericht korrekt, in der beantragten Änderung einen Verstoss gegen Art. 13 BGFA zu erkennen.[29] Das Urteil des Bundesgerichts zeigt, dass der Schutz des Berufsgeheimnisses vertraglich abgesichert werden muss und somit auch vertraglich abgesichert werden kann. Zudem hat das Bundesgericht klargestellt, dass die Haftung der Hilfsperson nicht auf vorsätzliches oder grob fahrlässiges Verhalten beschränkt werden darf. Einen allfälligen Haftungsausschluss der Anwaltskanzlei gegenüber ihrer Klientschaft hatte das Bundesgericht nicht zu beurteilen.

3. Strafrecht

Das anwaltliche Berufsgeheimnis ist auch durch das Strafrecht geschützt. Nach Art. 321 StGB werden Anwältinnen und Anwälte *sowie ihre Hilfspersonen,* die ein Geheimnis offenbaren, auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Das Geheimnis muss ihnen infolge ihres Berufes anvertraut worden sein, oder sie müssen es in dessen Ausübung wahrgenommen haben. Hier stehen drei Fragen im Zentrum: (1.) Unter welchen Voraussetzungen wird ein IT-Dienstleister zur Hilfsperson? (2.) Ist die Einwilligung der Klientschaft für das Hinzuziehen der Hilfsperson erforderlich? (3.) Wann ist das Tatbestandselement der Offenbarung erfüllt?

Für die Nutzung von Cloud-Diensten, deren Anbieter ihren Sitz in den USA haben, stellt sich zudem die Frage, welche Auswirkungen der amerikanischer CLOUD Act auf den Schutz des Berufsgeheimnisses hat.

Hilfsperson ist, «wer bei der Berufstätigkeit eines (Haupt-)Geheimnisträgers in einer Weise mitwirkt, die es ihr oder ihm grundsätzlich ermöglicht, von Geheimnissen Kenntnis zu nehmen».[30] Wenn ein IT-Dienstleister grundsätzlich keine Möglichkeit hat, die bei ihm liegenden Daten einer Anwältin zu lesen, ist er somit nicht Hilfsperson. Wenn die Daten unverschlüsselt auf dem Server des Dienstleisters liegen, kann er grundsätzlich davon Kenntnis nehmen und ist somit auch Hilfsperson.

Wenn ein IT-Dienstleister wegen der grundsätzlichen Möglichkeit, von Geheimnissen Kenntnis zu nehmen, Hilfsperson ist, stellt sich die Frage, ob für das Hinzuziehen dieser Hilfsperson die Einwilligung der Klientschaft erforderlich ist. Das Einholen einer solchen Einwilligung ist nicht notwendig, wird aber im Sinne einer zusätzlichen Absicherung generell[31] oder für bestimmte Konstellationen[32] empfohlen.

Art. 321 StGB ist ein Erfolgsdelikt. Die Strafbarkeit setzt somit voraus, dass eine unberechtigte Person tatsächlich Kenntnis vom Geheimnis erlangt hat. Die blosse Möglichkeit zur Kenntnisnahme genügt somit nicht. Das Abspeichern von Daten auch in unverschlüsselter Form erfüllt das Tatbestandselement der Offenbarung somit nicht. Das Berufsgeheimnis wird erst dann verletzt, wenn ein IT-Dienstleister tatsächlich Kenntnis von den Daten erlangt und zugleich nicht als Hilfsperson der Anwältin fungiert.

CLOUD Act steht für den amerikanischen Clarifying Lawful Overseas Use of Data Act, was mit Gesetz betreffend die Klarstellung der rechtmässigen Verwendung von Daten im Ausland übersetzt werden kann. Das Gesetz erlaubt es den US-Strafverfolgungsbehörden auf Bundesebene, Technologieunternehmen mit Sitz in den USA zu zwingen, Daten auch dann zur Verfügung zu stellen, wenn die verwendeten Server nicht in den USA stehen. Dies wirkt auf den ersten Blick höchst problematisch, bei genauerer Betrachtung zeigt sich jedoch, dass die Risiken meist überbewertet werden. Zunächst ist daran zu erinnern, dass der CLOUD Act nur für Strafuntersuchungen gilt und in jedem Fall einen Gerichtsbeschluss erfordert. Der Erlass zielt in erster Linie auf die Beschlagnahmung von Material im Ausland für Untersuchungen in den USA gegen sogenannte US-Personen ab.

Anwaltskollege David Rosenthal hat ein Modell zur Berechnung der Wahrscheinlichkeit eines Lawful Access im Ausland entwickelt und aufgezeigt, dass sieben (!) Voraussetzungen kumulativ erfüllt sein müssen, damit es zu einem Lawful Access durch eine ausländische Behörde kommen kann.[33] Um die Gesamtwahrscheinlichkeit eines Lawful Access zu berechnen, ist die Wahrscheinlichkeit für jede der sieben Voraussetzungen zu schätzen. Im von Rosenthal durchgerechneten Beispiel resultiert eine Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider von 0,67 Prozent in der (auf fünf Jahre festgelegten) Betrachtungsperiode. Das bedeutet, dass es in diesem Beispiel erst nach 513 Jahren mit einer Wahrscheinlichkeit von 50 Prozent zu einem erfolgreichen Lawful Access kommen würde. Für die genaue Berechnung und die Begründung der getroffenen Annahmen wird auf das Excel-Dokument von Rosenthal verwiesen.[34]

III. Beispiele für digitale Arbeitswerkzeuge

Die nachfolgenden Beispiele zeigen für gängige digitale Arbeitswerkzeuge, ob und, falls ja, wieso und unter welchen Voraussetzungen die Nutzung für Anwältinnen und Anwälte zulässig ist. Die Beispiele unterscheiden sich insbesondere durch das Vorhandensein von Ende-zu-Ende-Verschlüsselung sowie den Standort von Anbietern und Daten.

---

28 BGE 145 II 229 E. 7.5.
29 BGE 145 II 229 E. 7.6.
30 CHRISTIAN SCHWARZENEGGER ET AL., in: Anwaltsrevue 1/2019, S. 28.
31 CHRISTIAN SCHWARZENEGGER ET AL., in: Anwaltsrevue 1/2019, S. 30.
32 DAVID ROSENTHAL, [https://perma.cc/VET8-ZLH3 Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act], in: Jusletter 10. 8. 2020, Rz. 49 ff.
33 ROSENTHAL (Fn. 32), Rz. 109 ff.
34 DAVID ROSENTHAL, [https://perma.cc/D92U-GXGS Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden].

1. Digitale Ablage: Tresorit

Tresorit ist ein kostenpflichtiger Dienst der schweizerischen Tresorit AG, der das Speichern, Synchronisieren und Teilen von Dateien in der Cloud ermöglicht.[35] Anwaltskanzleien können damit ihre Daten wie beispielsweise Mandantendossiers digital ablegen. Alle Daten werden durch Ende-zu-Ende-Verschlüsselung geschützt, das heisst, Tresorit hat keinen Zugriff auf die Daten der Nutzerinnen und Nutzer. Vorteilhaft ist, dass die Daten nicht nur in der Cloud liegen, sondern lokal synchronisiert und damit bei Bedarf unabhängig von Tresorit gesichert werden können.

Die Nutzung von Tresorit ist für Anwältinnen und Anwälte in der Schweiz aus datenschutz-, anwalts- und strafrechtlicher Sicht ohne Weiteres zulässig. Der Dienst unterliegt vollumfänglich schweizerischem Recht, und die Daten liegen in der Schweiz. Tresorit erklärt ausserdem, die DSGVO einzuhalten. Für jene wenigen Daten, die nicht Ende zu Ende verschlüsselt werden können, zum Beispiel die Namen der Nutzer und die E-Mail-Adressen der Nutzerinnen, sodass eine Auftragsbearbeitung stattfindet, kann ein Auftragsverarbeitungsvertrag abgeschlossen werden.

2. Kanzleiverwaltung: Bexio

Bexio ist ein kostenpflichtiger Dienst der schweizerischen Bexio AG, der die Online-Verwaltung von Unternehmen wie beispielsweise Anwaltskanzleien ermöglicht.[36] Anwältinnen und Anwälte können damit unter anderem Projekte und die geleistete Zeit erfassen, ihre Buchhaltung führen und Rechnungen erstellen sowie ihre Kontakte verwalten.

Die Nutzung von Bexio ist für Anwälte in der Schweiz aus datenschutz-, anwalts- und strafrechtlicher Sicht grundsätzlich zulässig. Die Daten sind zwar nicht Ende zu Ende verschlüsselt, aber der Dienst unterliegt vollumfänglich schweizerischem Recht. Die Daten liegen zwar bei Google, aber in der Schweiz und im Verantwortungsbereich der Google *Ireland* Limited und nicht der *amerikanischen* Google LLC. Bexio erklärt, die DSGVO einzuhalten. Der Auftragsverarbeitungsvertrag, mit dem die Kontrolle der Nutzerinnen und Nutzer über ihre Daten vertraglich sichergestellt wird, ist Bestandteil der allgemeinen Geschäftsbedingungen (AGB).

3. Übersetzung: DeepL

DeepL ist ein Übersetzungsdienst der deutschen DeepL GmbH, der das Übersetzen von Texten in über einem Dutzend Sprachen ermöglicht. Als deutscher Dienst unterliegt DeepL der DSGVO und wird von der nordrhein-westfälischen Datenschutz-Aufsichtsbehörde beaufsichtigt. Die AGB stellen klar, dass die Rechte an ihren Daten bei den Nutzerinnen und Nutzern verbleiben.

DeepL kann kostenlos genutzt werden, doch ist die Bearbeitung von Personendaten bei dieser Version ausdrücklich untersagt.[37] Da Texte, die übersetzt werden sollen, häufig Personendaten enthalten, muss regelmässig die kostenpflichtige DeepL-Pro-Version genutzt werden. In dieser Version besteht die Garantie, dass Texte der Nutzerinnen nicht gespeichert, sondern sofort nach der Übersetzung gelöscht werden.[38] Der erforderliche Auftragsverarbeitungsvertrag ist sowieso nur für die DeepL-Pro-Version erhältlich.

Die Nutzung von DeepL ist für Anwältinnen und Anwälte in der Schweiz aus datenschutz-, anwalts- und strafrechtlicher Sicht in der kostenpflichtigen Pro-Version grundsätzlich zulässig. Das deutsche Datenschutzrecht einschliesslich DSGVO gewährt mindestens einen angemessenen Datenschutz, sodass der Datenexport aus der Schweiz zulässig ist. Die Daten zumindest aus den Übersetzungen werden nur kurzzeitig gespeichert und liegen in der Europäischen Union (EU).

4. Office: Microsoft 365

Microsoft 365 verbindet die traditionellen und lokal genutzten Microsoft-Office-Anwendungen wie Outlook und Word mit Cloud-Speichern, Cloud-Versionen der traditionellen Anwendungen sowie zusätzlichen Cloud-Diensten wie beispielsweise dem Zusammenarbeits- und Videokonferenztool Teams. Microsoft 365 ist ein Angebot der amerikanischen Microsoft Corporation, ermöglicht aber die Auswahl der Schweiz als Datenstandort.

Die Nutzung von Microsoft 365 ist für Anwältinnen und Anwälte in der Schweiz aus datenschutz-, anwalts- und strafrechtlicher Sicht zulässig, sofern beim Umstieg bestimmte technische, organisatorische und vertragliche Massnahmen zum Schutz der Datensicherheit und des Berufsgeheimnisses umgesetzt werden.[39] Es ist zu empfehlen, die getroffenen Massnahmen zu dokumentieren, um auf Verlangen einer Aufsichtsbehörde nachweisen zu können, dass insbesondere die Datensicherheit und das Berufsgeheimnis gewährleistet sind. Microsoft bietet unter anderem Anwaltskanzleien den Abschluss eines Professional-Secrecy-Addendums an. In diesem steht, dass Microsoft sich bewusst ist, dass Kundendaten unter das Berufsgeheimnis im Sinne von Art. 321 StGB fallen können. Indem Microsoft bestätigt, zu wissen, dass Daten eines bestimmten Kunden unter das Berufsgeheimnis fallen können, wird Microsoft zur Hilfsperson.

IV. Fazit

Gesetzgeber und Markt verlangen von der *gesamten* Anwaltschaft, mit der längst laufenden Digitalisierung mitzugehen und nicht länger stehen zu bleiben. Die Verwen-

35 [https://tresorit.com/de].
36 [https://www.bexio.com/de-CH/].
37 Vgl. [https://perma.cc/WS73-ZFLZ Datenschutzerklärung DeepL], Ziff. 3.
38 Vgl. [https://perma.cc/WS73-ZFLZ Datenschutzerklärung DeepL], Ziff. 4.
39 Für die detaillierte Begründung sei auf das Referat [https://youtu.be/OdJizFReYrQ «Kanzlei in der Cloud – wie es funktioniert»] von Anwaltskollege Christian Laux vom 11. 3. 2021 verwiesen.

dung moderner Software zwingt zum Schritt in die Cloud und dabei auch zur Nutzung von Cloud-Diensten im Ausland. Jüngere Mitarbeiterinnen und Mitarbeiter kennen nur noch die Arbeit mit solchen digitalen Arbeitswerkzeugen. Immer mehr Mandantinnen und Mandanten sind nur noch über digitale Kommunikationskanäle wie Instant Messaging und Social Media erreichbar.

Dieser Beitrag zeigt, dass der Weg zur digitalen Anwaltskanzlei und damit in die Cloud datenschutz-, anwalts- und strafrechtlich möglich ist. Dafür müssen entsprechende Beurteilungen und Diskussionen mit Blick auf die tatsächlichen Risiken geführt werden. Sogar der amerikanische CLOUD Act verliert seinen Schrecken, wenn man ihn nüchtern betrachtet. Umgekehrt verblasst der Glanz des Datenstandortes Schweiz, sobald man hinter die Kulissen des ausgebauten Überwachungsstaates blickt. Schliesslich muss berücksichtigt werden, dass der Verzicht auf digitale Arbeitswerkzeuge oder das Festhalten an alternder lokaler Software genauso mit Risiken verbunden ist.

Es ist zu wünschen, dass sich eine risikobasierte Betrachtung auch bei Aufsichtsbehörden und Gerichten durchsetzt. So wäre es beispielsweise problematisch, wenn Anwältinnen und Anwälte nur IT-Dienstleister beauftragen dürften, die auf die Beschränkung ihrer Haftung auf Vorsatz und grobe Fahrlässigkeit verzichten. Es stünden – wenn überhaupt – nur noch einige wenige IT-Dienstleister zur Auswahl, die weder funktional noch preislich konkurrenzfähig wären. Anwaltskanzleien und ihre nicht regulierte Konkurrenz benötigen gleich lange Spiesse. Ansonsten droht tatsächlich «The End of Lawyers», wie es Richard D. Susskind bereits 2008 in den Raum gestellt hat.[40]

40 Vgl. auch CHRISTIAN LAUX, [https://perma.cc/FS2W-G2FX The End of Lawyers? – Ableitungen aus Susskinds Thesen mit Blick auf IT in der Anwaltskanzlei], in: Anwaltsrevue 1/2015, S. 5 ff.