06.20

60. Jahrgang
Juni 2020
Seiten 161–192

StBp

Die steuerliche Betriebsprüfung

www.StBpdigital.de

Fachorgan für die Wirtschafts- und Prüfungspraxis

ESV ERICH SCHMIDT VERLAG

21019

Haftung des Steuerberaters bei Verletzung von Regelungen des Datenschutzrechts

Verletzung des Mandatsgeheimnisses durch Homeoffice?

*Rechtsanwältin, Fachanwältin für Handels-Gesellschaftsrecht Katja Wolpert, Frankfurt a. M./Mainz**

I. Einleitung

Gerade in Zeiten der Corona-Pandemie steigt die Relevanz der Beachtung und Einhaltung von Datenschutzregeln. Oft werden die drohenden Konsequenzen einer Missachtung der entsprechenden Vorschriften zu gering geschätzt, oft mangels Kenntnis der tiefgreifenden Wirkungen.

Steuerberater als wesentlicher Teil der steuerlichen Rechtspflege haben hierbei nicht nur die allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG)[1] und der Datenschutzgrundverordnung (DSGVO)[2] zu beachten, sondern diese auch im Lichte der sie berufsrechtlich zur besonderen Berufsverschwiegenheit verpflichtenden berufsrechtlichen Regeln (z. B. § 57 Abs. 1 StBerG[3], § 5 BOStB[4] und § 62 StBerG bei Gehilfen) zu beachten. Diese besondere berufliche Verschwiegenheitspflicht beeinflusst die sich durch das Datenschutzrecht ergebenden Abwägungskriterien zu Lasten des Steuerberaters.

Aus diesem Zusammenwirken ergibt sich für den Steuerberater nicht nur das in diesem Artikel im Weiteren näher behandelte Risiko eines Bußgeldes wie es anderen Unternehmern gleicher Größe und Umsatzstärke droht. Vielmehr muss der Steuerberater bei Verletzungen des Datenschutzes auch mit der Einleitung eines berufsrechtlichen und strafrechtlichen Verfahrens sowie dem Verlust seines Versicherungsschutzes rechnen.

Aktuell hat zwar eine Vielzahl von Corona-Gesetzen (so. z. B. das Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht v. 27. 3. 2020[5]) Verfahrensregeln vereinfacht. Eine Reduktion des Datenschutzniveaus ist bislang zu Gunsten der Steuerberater jedoch nicht erfolgt. Dabei ist es in Zeiten der Corona-Pandemie und des nun vielfältigen Einsatzes von Heimarbeitsplätzen (Homeoffice) schwieriger als zuvor, alle hierfür relevanten Aspekte zu beachten.

II. Datenschutz in der Steuerkanzlei

1. Der Datenschutz am Anfang des Mandatsverhältnisses

Das Datenschutzrecht beginnt mit der Mandatsbegründung. Dem Mandanten hierbei ein Massenmusterformular auszuhändigen, erfüllt bereits allein nicht die Voraussetzungen, die das Datenschutzrecht fordert.

So wird auch die Einwilligung des Mandanten zur Datenerhebung und Datenspeicherung nicht allein durch die Verwendung eines Massenmusterformulars, das durch Softwarebetreiber zur Verfügung gestellt wird, immer wirksam eingeholt.

Tatsächlich sind die Datenschutzpflichten weit umfangreicher und auch zeitlich darüber hinaus zu beachten. Öffentliche Stellen bieten hierzu inzwischen Vorlagen, Checklisten und „Standard-Datenschutzmodelle“[6] an, die auf die jeweilige Kanzlei und ihre Arbeitsabläufe angepasst werden müssen.

Aus Beweisgründen ist die Einwilligung des Mandanten in schriftlicher Form zu den Akten zu nehmen, um den jeweiligen Belehrungspflichten zu entsprechen und die drohende Unwirksamkeit einer Einwilligungserklärung weitgehend zu vermeiden. So scheitert eine wirksame Einwilligung teilweise bereits an Kleinigkeiten, so z. B. wenn der Einwilligende nicht weiß, gegenüber wem er eigentlich seinen Widerspruch erklären kann. Erwägungsgrund 42[7] stellt hierzu in Satz 4 klar, dass der Einwilligende mindestens darüber aufgeklärt worden sein muss, wer der „Verantwortliche“ ist.

Steuerberatungsgesellschaften fallen fast immer in den verschärften Anwendungsbereich des Datenschutzrechts, da sie mit jeder Gehaltsabrechnung und Einkommensteuererklärung, besonders zu schützende personenbezogene Daten[8] erheben und verarbeiten. Im Rahmen der Gehaltsabrechnung oder Einkom-

---

* Frau Rechtsanwältin Katja Wolpert ist seit über 20 Jahren im Bereich der Vertragsgestaltung von Unternehmen, gerade auch Freiberuflern, selbständig tätig und betreut diese auch in datenschutzrechtlicher Hinsicht.

1 Neufassung durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) v. 30. 6. 2017, BGBl. I 2017, 2097, zuletzt geändert durch das zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) v. 20. 11. 2019.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 v. 4. 5. 2016, 1.

3 Steuerberatungsgesetz, neugefasst durch Bekanntmachung der Neufassung des Steuerberatungsgesetzes (StBerG) v. 4. 11. 1975, BGBl. I 1975, 2735, zuletzt geändert durch das Gesetz zur Einführung einer Pflicht zur Mitteilung grenzüberschreitender Steuergestaltungen v. 21. 12. 2019, BGBl. I 2019, 2875.

4 Satzung über die Rechte und Pflichten bei der Ausübung der Berufe der Steuerberater und der Steuerbevollmächtigten – Berufsordnung (BOStB) i. d. F. v. 8. 9. 2010, *https://www.bstbk.de/downloads/bstbk/recht-und-berufsrecht/gesetze-und-verordnungen/BStBK_Berufsordnung.pdf*, zuletzt abgerufen am 20. 4. 2020.

5 BGBl. I 2020, 569.

6 Land Hessen: Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele, *https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/SDM-Methode_V2.0a_0.pdf zuletzt abgerufen am 20.4.2020*; ausführlicher hierzu: *Kehr/Zapp,* CB 2020, 100.

7 Erwägungsgründe des Europäischen Parlamentes und der Europäischen Kommission zur DSGVO, Erwägungsgrund Nr. 42, Satz 1, *https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html*, zuletzt abgerufen am 20. 4. 2020.

8 So die Regelung des Art. 9 DSGVO, auch in § 46 Nr. 14 BDSG.

mensteuerberechnung muss z. B. die für die Bestimmung der Kirchensteuer relevante Frage über „religiöse oder weltanschauliche Überzeugungen“ mit erhoben und gespeichert und auch Dritten (zumindest dem Veranlagungsfinanzamt) mitgeteilt werden.

Hiernach erforderlich ist die ausdrückliche Zustimmung zur Verarbeitung dieser Daten, konkludente Einwilligungen sind dem Gesetzeswortlaut nach gerade nicht ausreichend.[9] Damit ist in jedem Fall zu empfehlen, den Mandanten schriftlich über seine Rechte aufzuklären und sich die erfolgte Aufklärung ebenso schriftlich bestätigen zu lassen.

Bereits die Verarbeitung von Daten ohne Zustimmung des Betroffenen stellt einen sanktionsfähigen Datenschutzverstoß dar, der durch entsprechende Kanzleiorganisationsmaßnahmen vermieden werden sollte. Die Kanzlei muss alle möglichen und angemessenen technischen und organisatorischen Maßnahmen zum Schutz der Daten ergreifen.[10]

2. Kommunikation mit dem Mandanten

Auch die Kommunikation muss den Regeln Datenschutzrecht entsprechen. Das bedeutet zum einen, dass der Mandant insbesondere vorab einwilligen muss, dass eine Kommunikation per E-Mail, DropBox oder Cloud erfolgt. Auch hier sollte auf eine schriftliche ausdrückliche Einwilligung geachtet werden, um unnötige Risiken durch eine etwaig unwirksame Einwilligungserklärung zu vermeiden. Bei einer Speicherung und Verwendung einer Internet-Cloud ist sicherzustellen, dass hier eine vertrauenswürdige Speicherstelle verwendet wird.

Darüber hinaus ist jedoch auch nach Art. 32 DSGVO die Sicherheit der Verarbeitung zu prüfen und u. a. an die Erfordernisse der Daten anzupassen. Der Steuerberater muss hiernach ein „dem Risiko angemessenes Schutzniveau gewährleisten“.

Entscheidend ist, welche Risiken und mögliche Folgen eine Panne beim Datenschutz für die Betroffenen haben kann. Je höher das Risiko und die möglichen Folgen, umso stärker müssen die Sicherungsmechanismen sein, die eingeschaltet werden.

Da Steuerberater berufsmäßig immer mit Datenkategorien in Kontakt kommen (und durch etwa Gehaltsabrechnungen oder Einkommensteuerberechnungen versenden), die in den Bereich der besonders zu schützenden Datenkategorien[11] fallen, muss bei der Kommunikation und Übermittlung derartiger Daten ein besonders hohes Schutzniveau kanzleiintern geschaffen werden.

Dies wird auch durch die Abwägung gestützt, dass Steuerberater bei einer Datenpanne auch gleichzeitig dem Vorwurf der Verletzung ihrer Verschwiegenheitspflicht ausgesetzt sind.

Das Ziel eines Mandanten, z. B. durch Gestaltungsarbeiten auf legale und unproblematische Art und Weise Steuern einsparen zu wollen, wird dann gerade ad absurdum geführt, wenn die breite Öffentlichkeit (oder auch nur die Steuerverwaltung) bereits im Vorfeld über die Planung und Umgehungswege informiert wird. Die Abgabenordnung sieht hier u. a. vor, dass Umgehungsweisen als unwirksam angesehen werden und die Steuerpflicht nach der ursprünglich „richtigen“ Rechtsvorschrift zu berechnen ist.[12] Um derartige Risiken zu vermeiden ist die Übersendung von Informationen ausschließlich in verschlüsselter[13], nicht für jeden einsehbarer Form erforderlich.

Hierbei sollte eine aktuelle Änderung der Berufsordnung der Rechtsanwälte (BORA)[14] nicht außer Acht gelassen werden. In § 2 BORA wurde eine neue Regelung eingeführt, die die „Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, jedenfalls dann erlaubt, wenn der Mandant ihr zustimmt.“ Hierbei wird den Anwälten die Pflicht auferlegt, den Mandanten ausdrücklich vorab über die Risiken eines bestimmten Kommunikationsweges aufzuklären und seine Zustimmung einzuholen, bevor Informationen, die dem Mandatsgeheimnis unterliegen, über diesen Kommunikationsweg übermittelt werden.

Ob für die Steuerberater eine entsprechende Regelung verabschiedet werden wird, wird abzuwarten sein. Allein aus der Tatsache, dass den Rechtsanwälten hier eine besondere Ermächtigung im Rahmen ihrer Berufsordnung erteilt wurde, zeigt das erforderliche erhebliche Schutzniveau bei Verwendung digitaler Kommunikationswege.

Dass Daten per E-Mail nur noch verschlüsselt und durch ein angemessenes Passwort übermittelt werden dürfen, wird den Steuerberatern durch die von Steuerberatern meist bezogenen Softwareprodukte erleichtert.

III. Datenschutzpannen

Die Verletzung des Datenschutzes kann in zwei Fallgruppen aufgeteilt werden, durch den rechtswidrigen Eingriff von unberechtigten Dritten (also von außen) oder durch ein Fehlverhalten der Kanzlei des Steuerberaters (von innen).

1. Fallgruppe 1: Datenschutzverstoß durch Eingriff von „außen“

Das Risiko von Hackerangriffen steigt mit der Größe der Kanzlei und auch der Öffentlichkeitswirksamkeit ihrer Mandanten.

Veröffentlichte Hackerangriffe machen deutlich, wie aktuell dieses Thema gerade in Zeiten der Corona-Pandemie ist. So führte der Hackerangriff an der Universität Gießen im Dezember 2019 zu einem generellen Abschnitt der Universität vom Internet.[15] Auch am 31. 1. 2020 wurde von einem Hackerangriff gegen Lanxess berichtet.[16] Medien berichtete am 16. 3. 2020 über einen erfolgreichen Hackerangriff gegen die Online-Plattform Mebis, die eigentlich für den Fernunterricht in Bayern gedacht war.[17]

Der Steuerberater hat in jedem Fall technische Maßnahmen[18] (z. B. Firewall, angemessener Passwortschutz) zu ergreifen, um dieses Risiko weitgehend zu minimieren. Je „sensibler“ die entsprechenden Daten sind, desto intensiver und umfangreicher sind die Maßnahmen, die zum Schutz der Daten zu ergreifen sind.

2. Fallgruppe 2: Datenschutzverstoß durch Handeln von „innen“

Das Risiko, dass ein Datenschutzverstoß durch die Kanzlei selbst erzeugt wird, besteht unabhängig von der Kanzleigröße.

9 So § 51 Abs. 5 BDSG, Art. 9 Abs. 2 lit. a DSGVO.
10 So § 9 BDSG.
11 S. Art. 9 DSGVO, § 22 BDSG.
12 So § 42 AO.
13 So auch der Wortlaut des § 22 Abs. 2 Nr. 7 BDSG.
14 In der Fassung v. 1. 1. 2020, zuletzt geändert durch Beschluss der Satzungsversammlung v. 6. 5. 2019, *https://brak.de/w/files/02_fuer_anwaelte/berufsrecht/bora_stand_01.01.2020.pdf*, zuletzt abgerufen am 20. 4. 2020.
15 *https://www.hessenschau.de/panorama/moeglicher-hackerangriff-legt-uni-giessen-lahm,uni-giessen-vom-netz-100.html*, zuletzt abgerufen am 20. 4. 2020
16 *https://www.tagesschau.de/investigativ/ndr/hackerangriff-chemieunternehmen-101.html*, zuletzt abgerufen am 20. 4. 2020.
17 *https://www.faz.net/aktuell/karriere-hochschule/fernunterricht-wegen-corona-bayerische-lernplattform-gehackt-16681312.html*, zuletzt abgerufen am 20. 4. 2020.
18 So auch in § 9 BDSG formuliert.

Steuerberater müssen bereits aufgrund berufsrechtlicher Regelungen (§ 62 StBerG) auf die Einhaltung von Verschwiegenheitsregeln hinwirken und belehren. Die „Scharfschaltung" der DSGVO zum 25. 05. 2018 hat hier zu einer erneuten Überarbeitung und Bewusstmachung der Pflichten geführt.

Auch beim Einsatz von Kommunikationssoftware hat der Steuerberater sorgfältig die Datensicherheit zu prüfen. Den meisten Steuerberatern ist die Verwendung von „WhatsApp" oder „Skype" bekannt, wie auch der Tatsache, dass viele Unternehmen (u. a. Continentale, BMW und VW) sich im Jahr 2018[19] aufgrund der Regelungen der DSGVO entschieden haben, die Verwendung von „WhatsApp" auf beruflich genutzter Hardware strikt zu untersagen, um die Übermittlung von Daten wie Name, Mobilfunknummer, Nutzungsdaten, Standortdaten, Kontaktdaten und Nachrichten-Informationen und die damit verbundene Verletzung von Geheimhaltungspflichten zu vermeiden.

Auch wenn der Mandant auf der Verwendung einer derartigen Software besteht, bei der der Steuerberater seinerseits nicht sicherstellen kann, dass die von ihm übermittelten Informationen nicht doch einer breiteren Öffentlichkeit bekannt werden, sollte der Steuerberater hier die Risiken genau abwägen und im Zweifel eine sicherere Kommunikation bevorzugen.

In jedem Fall sollte er den Mandanten ausdrücklich und nachweisbar über die drohenden Risiken vorab informieren und hierauf folgend dessen Einwilligung einholen, bevor er diese Medien nutzt und sich von seinem Mandanten von hieraus resultierenden Haftungsrisiken freistellen lassen.[20]

Auch im Falle der Vorlage einer solchen Einwilligung und Haftungsfreistellung sollte der Steuerberater abwägen, ob er das Risiko tatsächlich eingeht.

Bei Verstoß gegen den Datenschutz und der Veröffentlichung von persönlichen Daten des Mandanten und damit einhergehender Verletzungen der Verschwiegenheitspflicht kann mit der Einwilligung zwar u. U. der Schadensersatzanspruch des Mandanten beschränkt oder abgewehrt werden.

Ob hierdurch die anderen Sanktionen abgewehrt werden können, hängt vom Einzelfall ab. Sowohl die Datenschutzgesetze als auch das Strafgesetzbuch sanktionieren die Rechtsverletzung unabhängig voneinander mit einem Bußgeld oder stärkeren Sanktionen. Die Steuerberaterkammern ihrerseits dürfen bei der Entscheidung über die zu ergehende Sanktion auch auf das Berufsbild abstellen, auf die Wirkungen des Verstoßes auf die Allgemeinheit und vor allem auf das Vertrauen der Allgemeinheit in die steuerberatenden Berufe.[21]

IV. Besondere Herausforderungen des Datenschutzes im Homeoffice

1. Allgemeines

Die aktuelle Situation mit der Verlagerung der Tätigkeiten ins „Homeoffice" führt dazu, die Einhaltung des Datenschutzrechts und den besonderen Schutz des Mandatsgeheimnisses neu zu überprüfen. Hierbei sind neben dem Datenschutz auch viele andere Aspekte zu beachten.[22] Hieraus folgend müssen dann neben den technischen auch die organisatorischen Maßnahmen[23] angepasst werden, sowie neue Handlungsanweisungen für die Mitarbeiter erstellt werden, um dem erforderlichen berufsrechtlichen und datenschutzrechtlichen Schutzniveau zu entsprechen. Soweit Steuerberater oder ihre Mitarbeiter im Homeoffice tätig sind, erhöht sich das Risiko eines Datenschutzverstoßes erheblich und damit verbunden auch die Handlungs- und Belehrungspflichten des Steuerberaters, u. a. da im Homeoffice eine Vielzahl an Risiken für die Realisation von Datenschutzverstößen lauern, die im Rahmen der Tätigkeit in den Räumen der Kanzlei aufgrund der technischen Infrastruktur und auch der räumlichen Abgeschlossenheit nicht vorhanden sind.

Auch wenn der Mitarbeiter im Homeoffice arbeitet, haftet der Steuerberater als „verantwortliche Stelle" für alle begangenen Datenschutzverstöße höchst persönlich.[24]

2. Einzelne Fallgruppen

An dieser Stelle sind verschiedene Aspekte zu beachten. Auf ein paar soll im Folgenden eingegangen werden:

- Nutzung eines beruflichen Computers[25] auch zu privaten Zwecken
  Bei der Überlassung eines beruflichen Computers ist zuerst zu entscheiden, ob dem Mitarbeiter die private Nutzung erlaubt oder ausdrücklich untersagt wird. Hier sind entsprechende Regelungen und Schutzmaßnahmen softwaretechnisch einzubinden.
  Unabhängig davon ist bei der Durchführung von Arbeiten am kanzleieigenen Computer von zu Hause aus sicherzustellen, dass ein unbeabsichtigter „Zugriff" durch Ehepartner und auch Kinder durch Installieren eines Passwortschutzes und Verwendung eines passwortgeschützten Bildschirmschoners bei Verlassen des Computers – auch nur für eine kurze Zeit – vermieden wird.
  Für eine Erleichterung zur Kontrolle der Einhaltung der Pflichten durch den Arbeitgeber hat nun die Entscheidung des Bundesarbeitsgerichts geführt, so dass der Steuerberater Einsichtnahme auf den Dienstrechner des Mitarbeiters nehmen darf, soweit die Dateien nicht als „privat" gekennzeichnet wurden.[26]
- Nutzung eines privaten Computers auch zu beruflichen Zwecken
  Soweit private Computer verwendet werden, verfügen diese oft nicht über aktuellen Virenschutz oder Firewalleinstellungen. Teilweise ist auf dem Computer bereits eine Spy-Software installiert, vielleicht durch Öffnen eines unbekannten E-Mailanhangs durch Kinder oder durch Installation eines fremden Softwareprogramms.
  Vielen Nutzern ist nicht bewusst, welche Informationen diverse Softwareprogramme an die Hersteller versenden, ohne die Nutzer hierüber – außer in den AGB – zu informieren. Soweit der Computer auch zu beruflichen Zwecken genutzt wird, obliegt dies der Eigenverantwortung der Nutzer und im Falle der Veröffentlichung der Daten, der Haftung des Steuerberaters. Er kann seine Haftung nur insoweit zu be-

19 *https://www.manager-magazin.de/unternehmen/autoindustrie/continental-whatsapp-und-snapchat-auf-diensthandys-verboten-a-1211215.html*, zuletzt abgerufen am 20. 4. 2020, so auch: *https://www.t-online.de/digital/id_83881114/whatsapp-erste-firma-verbietet-die-chat-app-auf-diensthandys.html*, zuletzt abgerufen am 20. 4. 2020.

20 In Anlehnung an die neue Regelung in § 2 BORA.

21 So in § 89 StBerG.

22 Das Handelsblatt hat eine grobe 6-Punkte-Checkliste hierzu herausgegeben, abrufbar unter *https://www.handelsblatt.com/unternehmen/beruf-und-buero/buero-special/rechtslage-im-home-office-6-punkte-checkliste-fuer-das-home-office/13732676-2.html?ticket=ST-1386963-CgFb5YjYS472TdZByJOo-ap2*, zuletzt abgerufen am 20. 4. 2020.

23 So auch in § 9 BDSG formuliert.

24 § 46 Nr. 7 BDSG, Art 4 Nr. 7 DSGVO.

25 Hier und in der Folge als Oberbegriff verwendet für Laptop, Tablet und sonstige genutzte Hardware.

26 BAG v. 31. 1. 2019 2 AZR 426/18, bislang nur abrufbar unter *http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=22507*, zuletzt abgerufen am 22. 4. 2020.

grenzen versuchen, in dem er dem Mitarbeiter entsprechende Handlungsanweisungen erteilt und ein Bewusstsein für die Verschwiegenheitspflicht auch im privaten Umfeld schafft.

- Allgemeine Risiken zu Hause
  Hinzu kommen andere Risiken, die in den kanzleieigenen Räumen durch andere organisatorische Maßnahmen ausgeschlossen werden können.
  Wie z. B.
  - Das Ausdrucken mandantenbezogener Daten und Liegenlassen im Druckerschacht.
  - Das Verwenden von Fehlausdrucken als Schmierpapier.
  - Entsorgung von Fehlausdrucken oder Skizzen im Papierkorb oder Hausmüll.
- Laufende Überwachung
  Sobald ein Computer in privaten Räumen auch dem tatsächlichen Zugriff von Familienmitgliedern unterliegt, ist bei den Nutzern besonderes Bewusstsein zu schaffen. Zu vermeiden ist, dass der Computer unkontrolliert Kindern oder mit den Grundsätzen des Datenschutzes (zusammen mit bestehenden Verschwiegenheitspflichten) nicht vertrauten Familienangehörige überlassen wird. Dies schon, um die versehentliche Installation von Spy-Software sowie Softwarekomponenten, die unkontrollierbar Informationen übertragen, zu unterbinden.
- Verwendung eines Videokonferenzsystems
  Im Rahmen der Corona-Pandemie wird nun auch die Nutzung diverser Konferenzsoftware immer aktueller. Die Videokonferenzsoftware muss eine datensichere Übertragung an den Mandanten sicherstellen.
  Auch hier sollte genau darauf geachtet werden, welche Software zum Einsatz kommt. Aktuell in der Presse erscheint hier als Negativbeispiel die Software „Zoom". Am 1. 4. 2020 hat die Tagesschau[27] darüber berichtet, dass sich die New Yorker Staatsanwaltschaft eingeschaltet und Ermittlungen gegen den Betreiber aufgenommen hat, aufgrund diverser begründeter offizieller Beschwerden von Datenschützern.
  Heise[28] hatte bereits seit März 2020 immer wieder vor der Verwendung dieser Software gewarnt, weil z. B. die Software bei ihrem Start Daten an Facebook sandte, unabhängig davon, ob der Nutzer ein Facebook-konto besaß oder nicht. Es wurde in der Folge berichtet, dass durch Zoom ermittelte personenbezogene Daten im Darknet zum Kauf angeboten wurden.
  Der Steuerberater ist gehalten, Software vor deren erstmaliger Installation und Verwendung dahingehend zu prüfen, ob diese Software den erforderlichen Datenschutz beachtet. Aufgrund der leichten Erreichbarkeit derartiger Informationen im Internet, auch für Laien, begründet die Nichtdurchführung einer Recherche den Fahrlässigkeitsvorwurf bei der Datenschutzverletzung und der Verletzung der beruflichen Verschwiegenheitspflicht.
  Weiterhin muss der Nutzer bei Verwendung einer Korrespondenzsoftware die Medienberichte verfolgen und beständig die Verwendung seiner Kommunikationssoftware reflektieren und eine neue Risikoanalyse dahingehend durchführen, ob er die konkrete Software weiterhin nutzen darf.
  Oben war bereits zur Frage Stellung genommen worden, wie der Steuerberater mit dem Verlangen eines Mandanten umgehen sollte, eine bestimmte Software zu verwenden.
- Verwendung einer Webcam
  Die Nutzung einer Webcam stellt den Steuerberater hinsichtlich seiner Mitarbeiter vor neue Herausforderungen. Insoweit ist ein Datenschutz sowohl gegenüber dem Mitarbeiter als auch gegenüber dem Mandanten zu beachten.
  Zum Schutz der Privatsphäre des Mandanten ist der Mitarbeiter daher im Rahmen von Handlungshinweisen darauf zu sensibilisieren, nicht im Rahmen der Webcam Nutzung private personenbezogene Daten zu übermitteln. Hierzu gehören auch Selbstverständlichkeiten, wie das Urlaubsfoto mit den Urlaubsdaten, das im Hintergrund an der Wand hängt.
  Sowohl zum Schutze der Mitarbeiter als auch der Mandanten ist der Mitarbeiter anzuweisen, die Webcam zu deaktivieren, wenn sie nicht benötigt wird. Hierdurch soll das Risiko minimiert werden, dass personenbezogenen Daten durch eine Software erfasst und mittels der Webcam (Bild und Ton) übermittelt werden ohne ausdrücklichen Willen der im Raum anwesenden Personen.
  Weitere technische Maßnahmen (Einstellungen) sind zu beachten. So ist eine etwaig vorhandene Überwachungsfunktion der Webcam zu deaktivieren.

3. Checkliste

U. a. sollte der Steuerberater bei nun aktueller Überarbeitung der durch das Datenschutzrecht verlangten TOMs[29] folgende Fragen abwägen und dokumentiert für die jeweilige Datenschutzbehörhörde archivieren:

1) Ist mein Mitarbeiter für den Schutz personenbezogener Daten hinreichend sensibilisiert?
2) Ist in der Handlungsanweisung der Mitarbeiter eine Passage für das Aufstellen des Computers und der Nutzung der Webcam enthalten?
3) Wechselt der Mitarbeiter öfter den Tätigkeitsort? Ist der sichere Transport der Hardware in der Handlungsanweisung enthalten?
4) Hat der Mandant der Verwendung der digitalen Medien/der konkreten Kommunikationssoftware zugestimmt?
5) Hat der Mitarbeiter der Speicherung seiner personenbezogenen Daten etc. im Homeoffice zugestimmt?
6) Befindet sich auf dem Computer eine aktuelle Virensoftware? Wird die Festplatte regelmäßig nach Viren und Spy-Software gescannt?
7) Ist die verwendete Software auf dem Computer datensicher verwendbar? Wie oft wird die Entscheidung der Verwendung der konkreten Software reflektiert.
8) Welche weitere Hardware darf an den Computer angeschlossen werden (Drucker, Handy)? Ist dies in der Handlungsanweisung des Mitarbeiters abgebildet?
9) Ist die Webcam deaktiviert, wenn sie nicht benötigt wird?
10) Ist der W-LAN Zugang mit einem sicheren Passwort geschützt?
11) Wird ein „öffentliches Netzwerk" verwendet?
12) Ist der Firmenzugang (z. B. VNC) wirklich datensicher?
13) Wird nur die Kanzlei-E-Mail-Adresse für die Übertragung von Mandantendaten genutzt?
14) Werden die Kanzleidaten ausschließlich auf dem Server der Kanzlei gespeichert?
15) Ist bei Speicherung in der Cloud der Datenschutz weiterhin gewährleistet?
16) Erfolgt bei Speicherung auf dem genutzten Computer eine automatische Sicherung (Backup) der Daten?

27 *https://www.tagesschau.de/ausland/zoom-101.html*, zuletzt abgerufen am 20. 4. 2020.
28 *https://www.heise.de/security/meldung/Videokonferenz-Software-Ist-Zoom-ein-Sicherheitsalptraum-4695000.html*, zuletzt abgerufen am 20. 4. 2020.
29 Technische und organisatorische Maßnahmen wie in § 9 BDSG und Art. 32 DSGVO aufgeführt.

V. Die Konsequenzen eines Datenschutzverstoßes

1. Meldepflicht

Nach § 65 Abs. 1 BDSG (Art. 33 Abs. 1 DSGVO) sind Datenschutzpannen unverzüglich der zuständigen Behörde gegenüber zu melden, spätestens innerhalb von 72 Stunden nach Bekanntwerden. Das entsprechende Konzept für den Eintritt einer Datenschutzpanne hatte jede Kanzlei bereits seit 2018 aufzustellen inklusive Folgenabschätzung. Diesem Protokoll ist nun zu folgen.

Die Unterlassung dieser Meldepflicht kann zur Sanktionierung durch die Erhebung oder Erhöhung von Bußgeldern führen.

2. Bußgelder

§ 83 BDSG (Art. 83 Abs. 2 DSGVO) enthält einen Katalog für Bemessungskritierien, der für die Höhe des festzulegenden Bußgeldes heranzuziehen ist. Hierzu gehören neben Art, Schwere und Dauer des Verstoßes auch das Verschuldensmaß (Vorsatz oder Fahrlässigkeit) hinsichtlich des eingetretenen Verstoßes und der Grad der Verantwortung im Hinblick auf die eingeführten technischen und organisatorischen Maßnahmen.[30]

Die Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hatte bereits am 14. 10. 2019 ein Konzept entwickelt, um die Bußgelder der Höhe nach bestimmen zu können.[31] Kernaussage dieses Konzeptes ist, dass sich die Höhe des Bußgeldes nach fünf Schritten berechnen lässt, das sich einerseits konkret durch Werte des konkreten Unternehmens, andererseits aufgrund von Durchschnittswerten berechnen lässt. Maßgeblich sind insbesondere die Größe des Unternehmens und auch dessen jeweiligen Jahresumsatzes. Es wird vielfach vermutet, dass dieser Bußgeldkatalog zu deutlich höheren Bußgeldern führen wird.[32]

Bereits im Dezember 2019 berichtete das Handelsblatt[33], dass gegen 1&1 ein empfindliches Bußgeld in Höhe von 9,6 Millionen Euro verhängt wurde, da Kundendaten am Telefon an unberechtigte Nutzer weitergegeben wurden.

Der Landesbeauftragte für Datenschutz des Landes Brandenburg berichtet in seinem Tätigkeitsbericht von 2019 von einem Bußgeld in vierstelliger Höhe, das gegen einen Mediziner verhängt wurde, dessen Freund die Datensicherung von Patientendaten auf seinem anderweitig beruflich genutzten Computer speicherte (ohne Auftragsverarbeitungsvereinbarung), wo sie der Arbeitgeber des Freundes fand.[34]

Dass sich die Situation im Bereich der DSGVO-Bußgelder allgemein verschärft, zeigen diverse Übersichten, die im internet frei zugänglich sind.[35]

Besonderer Fall der Erschwerung im Homeoffice:

Relevanter Ermessensgrund für die Höhe des Bußgeldes ist nach Art. 83 Abs. 2 Nr. 4 DSGVO auch der Grad der Verantwortung im Hinblick auf die technischen und organisatorischen Maßnahmen.[36] Wenn somit der Steuerberater seinen Mitarbeitern die Arbeit im Homeoffice gestattet, ohne sie auf die besonders zu beachtenden Maßnahmen in nachweisbarer Form aufgeklärt zu haben, muss er mit einem höheren Anteil an der Verletzung des Datenschutzes und somit einem höheren Bußgeld rechnen.

3. Schadensersatzansprüche nach DSGVO

Jeder Betroffene kann einen Schadensersatzanspruch aufgrund der Regelung des § 83 BDSG[37] gegenüber der Steuerberatungskanzlei geltend machen. Hierfür ist zwar der konkrete Nachweis eines entstandenen Schadens (Kausalität und Schadenshöhe) nach bisheriger Rechtsprechung[38] erforderlich, das Verschulden der Steuerberaterkanzlei wird jedoch weiterhin vermutet.

Von vielen bislang unbeachtet geblieben ist aber auch die Möglichkeit des Mandanten, ein „Schmerzensgeld“ wegen des Datenschutzverstoßes zu verlangen.[39] Der Mandant, der aufgrund seiner öffentlich übermittelten Einkommenssituation in Angst verfällt, einem Shitstorm[40] ausgesetzt zu sein, kann hier zusätzlich Ansprüche in erheblichem Umfang geltend machen.

4. Strafbarkeit

Die Verletzung der berufsrechtlichen Verschwiegenheit ist nach § 203 Abs. 1 Nr. 3 StGB mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe sanktionierbar. Wie hoch die Pflichten zur Beachtung der beruflichen Verschwiegenheitspflicht des Steuerberaters einzustufen sind, ergibt sich nicht erst durch das Strafgesetzbuch.

Das Bundesverfassungsgericht hat wiederholt in seiner Rechtsprechung die Bedeutung des Steuerberaters als Teil der „freien Advokatur“ der rechtsberatenden Berufe deutlich gemacht.[41] Die Anwendung des § 203 Abs. 1 Nr. 3 StGB wurde erst wieder gestärkt, in dem die Steuerberaterkammer zusammen mit dem Steuerberaterverband im Januar 2019 im Rahmen einer Veröffentlichung, in dem sie den Richtlinienvorschlag der Europäischen Kommission[42] unterstützte, die Relevanz der Verschwiegenheitspflicht und des Vertrauens des Mandanten hierauf herausstellte und erklärte, dass auch Steuerberater von der Verpflichtung zur Offenbarung („Whistleblower“) zu befreien sind.

5. Berufsrechtliche Konsequenzen

Steuerberater sind nach den berufsrechtlichen Regelungen[43] zur Verschwiegenheit als eine der maßgeblichen Grundelemente der Steuerberatertätigkeit und des Mandantenschutzes verpflichtet. Eine Verletzung dieser Pflichten allein kann bereits – ja nach Schwere der Schuld – zur Einleitung eines berufsrechtlichen Verfahrens führen.

Hierfür werden bei den ordentlichen Gerichten gesonderte Kammern durch Berufsrichter geführt. Entgegen der strafrechtlichen Frage der Erfüllung des Straftatbestandes und der Stärke der Schuld ist hier vor allem auch entscheidungserheblich, ob das Verhalten des Steuerberaters geeignet ist, in der Öffentlichkeit das Ansehen des Berufsstandes zu schädigen.[44] Entscheidend bei

30 So auch in § 9 BDSG formuliert.
31 *https://www.heise.de/security/meldung/Videokonferenz-Software-Ist-Zoom-ein-Sicherheitsalptraum-4695000.html*, zuletzt abgerufen am 20. 4. 2020.
32 *Wybitul/Celik,* ZRFC 2020, 22 (25).
33 *https://www.handelsblatt.com/politik/deutschland/dsgvo-datenschutz-verstoesse-zahl-der-bussgelder-ist-drastisch-gestiegen/25364576.html?ticket=ST-1111989-vvBwPXB1LzuaaVqRr4Aj-ap1*, zuletzt abgerufen am 20. 4. 2020.
34 *https://www.lda.brandenburg.de/media_fast/4055/TB_2019_Datenschutz.pdf* Seite 31, Punkt 8.3. zuletzt abgerufen am 20. 04. 2020.
35 *https://www.heise.de/newsticker/meldung/DSGVO-Bislang-75-Bussgelder-wegen-Verstoessen-4420368.html*; *https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php*, zuletzt abgerufen am 20. 4. 2020
36 So auch in § 9 BDSG formuliert.
37 Gleichlautend Art. 82 Abs. 1 DSGVO.
38 AG Bochum v. 11. 3. 2019 65 C 485/18, FamRZ 2019, 1182–1183; LG Karlsruhe v. 2. 8. 2019 8 O 26/19, ZD 2019, 511–512.
39 § 83 Abs. 2 BDSG, Artz. 82 Abs. 2 DSGVO.
40 Näher ausgeführt u. a. durch das Sat1-Portal, *https://www.sat1.de/ratgeber/sicherheit-im-internet/was-ist-ein-shitstorm*, zuletzt abgerufen am 20. 4. 2020.
41 BVerfG v. 30. 3. 2004 2 BvR 1520/01, 2 BvR 1521/01, Rn. 100; v. 12. 4. 2005 2 BvR 1027/02, Rn. 94; v. 13. 6. 2007 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05, Rn. 163.
42 *https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-218-F1-DE-MAIN-PART-1.PDF* zuletzt abgerufen am 20. 4. 2020.
43 Vor allem § 57 Abs. 1 StBerG, § 5 BOStB.
44 §§ 89 Abs. 2, 92 StBerG.

den Abwägungen ist auch insbesondere die Wahrung des Vertrauens „aller Rechtssuchenden“ in die Integrität der Zunft der Steuerberater. Dies kann bis zur Entziehung der Steuerberaterzulassung führen.[45]

Sollte ohne ausdrückliche Beschwerde ein Strafverfahren eingeleitet werden, das z. B. zu einer Klageerhebung führt, so ist die Steuerberaterkammer automatisch hiervon zu informieren (Nr. 24 MiStra Abs. 1, 3. Spiegelstrich[46]), so dass die Einleitung eines berufsrechtlichen Verfahrens in jedem Fall droht.

VI. Fazit

Die Einhaltung datenschutzrechtlicher Regelungen mag bei Mandatsbegründung den für den Steuerberater relevanten Schwerpunkt bilden. Jedoch ist dies auch während der Mandatsbetreuung und der gewählten Art der Kommunikation ebenso zu beachten. Dies hat bei der Arbeit von zu Hause gleiche Relevanz, wobei man neben den Risiken von „außen“, vor allem auch die Risiken aus der eigenen Tätigkeit und der Tätigkeit der Mitarbeiter, somit von „innen“ nicht vernachlässigt werden dürfen. Hinzu kommen im Übrigen zusätzliche Risiken, die im Vorfeld bedacht und geregelt werden sollten, um die besonders schwerwiegenden Sanktionsrisiken bei Nichtbeachtung der Regeln und Eintritt eines Schadens minimieren zu können.

45 § 90 StBerG.
46 Anordnungen über Mitteilungen in Strafsachen v. 27. 3. 2019, BAnz AT 08. 04. 2019 B 1.