Kleemann/Kader: EU-Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

DStR 2018, 1091

EU-Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

Praktische Umsetzung des neuen Datenschutzrechts in kleinen und mittelständischen Steuerberatungskanzleien

Roland Kleemann und Martin Kader*

In der Büroorganisation der Steuerberatungskanzleien spielt der Schutz personenbezogener Daten schon wegen des Berufsgeheimnisses eine hervorgehobene Rolle. Bislang hatten die Kanzleien bereits nach dem Bundesdatenschutzgesetz (BDSG aF) zahlreiche datenschutzrechtliche Pflichten. Ab dem 25.5.2018 müssen die neuen Vorschriften der Datenschutz-Grundverordnung (DSGVO) angewendet werden. Der vorliegende Aufsatz bietet einen Überblick über die wichtigsten Maßnahmen zur Anpassung der Datenverarbeitung der Kanzlei an das neue europäische Datenschutzrecht.

1. Einleitung

Die am 25.5.2016 in Kraft getretene DSGVO gilt nach einer zweijährigen Übergangszeit seit dem 25.5.2018 unmittelbar. Daneben müssen die neuen Vorschriften des deut-

schen Bundesdatenschutzgesetzes (BDSG) beachtet werden, das der Gesetzgeber mit dem DSAnpUG-EU v. 30.6.2017[1] an die DSGVO angepasst hat. Zwar gelten EU-Verordnungen grundsätzlich vorrangig vor dem nationalen Recht. Jedoch lässt die DSGVO in sog. Öffnungsklauseln zahlreiche Spielräume, die es den Mitgliedstaaten der EU ermöglichen, Detailregelungen im nationalen Recht zu erlassen.[2]

Viele der konkreten Anforderungen, wie beispielsweise die technischen und organisatorischen Maßnahmen (TOM) für die Verarbeitungssicherheit, bestimmen bereits nach dem BDSG seit längerer Zeit die Büroorganisation aller datenverarbeitenden Stellen. Für den Berufsstand des Steuerberaters liegt die Bedeutung des neuen EU-Datenschutzrechts vor allem in den erhöhten Pflichten zur Dokumentation, der Transparenz gegenüber betroffenen Personen und Aufsichtsbehörden sowie in der Haftung und Sanktionierung bei Verstößen gegen den Datenschutz. Gerade kleine und mittelständische Steuerberatungskanzleien müssen ihre Datenverarbeitungsprozesse mit vertretbarem Aufwand an die neuen Normen anpassen. Dabei kann eine effiziente und zukunftsgerichtete Datenschutzorganisation mit zahlreichen Vorteilen für die Kanzlei verbunden sein. Der Schutz personenbezogener Daten wird in Zeiten von zunehmender Digitalisierung und Cyberangriffen immer bedeutsamer und kann als Qualitätsmerkmal und Instrument der Mandantenbindung verstanden werden.

Momentan erscheinen eine Vielzahl von Publikationen zu allgemeinen Themen des neuen EU-Datenschutzrechts. Die BStBK und der DStV e.V. haben Hinweise speziell zur Umsetzung für Steuerberater entwickelt, die vornehmlich auf die Bedürfnisse der kleinen und mittleren Kanzleien

abgestimmt sind.[3] Im Folgenden werden begleitend zu den Hinweisen die wichtigsten Umsetzungsmaßnahmen praxisnah hervorgehoben und erläutert.

2. Die wichtigsten Umsetzungsmaßnahmen

2.1 Datenschutz-Leitfaden und IT-Sicherheitskonzept

Gemäß Art. 5 Abs. 2 DSGVO muss der Verantwortliche (idR Inhaber der Kanzlei) die Einhaltung der in Art. 5 Abs. 1 DSGVO formulierten Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können. Es bietet sich an, die nachstehenden Verarbeitungsgrundsätze[4] einschließlich des IT-Sicherheitskonzepts in einem Datenschutz-Leitfaden zu dokumentieren.

2.1.1 Grundsatz der „Rechtmäßigkeit" der Verarbeitung

Jede Verarbeitung bedarf einer Rechtsgrundlage, die zu Nachweiszwecken einmal dokumentiert werden sollte. Häufig vorkommende Rechtsgrundlagen sind zB die folgenden:

- Art. 6 Abs. 1 S. 1 Buchst. b DSGVO für die Verarbeitung der Mandantendaten zum Zwecke der Erfüllung des Steuerberatungsvertrages,
- Art. 6 Abs. 1 S. 1 Buchst. c DSGVO zur Erfüllung einer rechtlichen Verpflichtung des Steuerberaters, etwa zur Aufbewahrung von Handakten nach dem StBerG usw,
- Art. 6 Abs. 1 S. 1 Buchst. f DSGVO zur Wahrung berechtigter Interessen des Steuerberaters oder eines Dritten, zB zur Durchsetzung von Vergütungsansprüchen des Steuerberaters, von personenbezogenen Daten der Debitoren und Kreditoren in der Finanzbuchhaltung,
- Art. 6 Abs. 1 S. 1 Buchst. a DSGVO und bei Einwilligung der betroffenen Person: zB die Einwilligungserklärung eines Mandanten oder sonstigen Interessenten beim Bezug eines Newsletters.

Zur Verarbeitung besonderer Datenkategorien iSv Art. 9 DSGVO, den sog. sensiblen Daten, bedarf es einer besonderen Rechtsgrundlage.[5] In der Steuerberatungspraxis können von diesen besonderen Datenkategorien insbesondere Religionsdaten, Gewerkschaftszugehörigkeiten, Gesundheitsdaten, Daten über die sexuelle Orientierung (zB eingetragene Lebenspartnerschaften) und biometrische Daten (zB Fotos) relevant werden.[6] Häufig vorkommende Rechtsgrundlagen zur Verarbeitung dieser sensiblen Daten sind:

- Art. 9 Abs. 2 Buchst. a DSGVO für die Verarbeitung personenbezogener Daten mit ausdrücklicher Einwilligung der betroffenen Person (zB die Veröffentlichung des Fotos eines Mitarbeiters auf den Kanzleiwebseiten),
- Art. 9 Abs. 2 Buchst. f DSGVO für die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- § 26 Abs. 3 BDSG für die Verarbeitung von sensiblen Daten der Beschäftigten des Mandanten im Rahmen der vom Steuerberater übernommenen Lohn- und Gehaltsbuchführung (zB Krankmeldungen, Konfession des Mitarbeiters etc); die Rechtsgrundlage des § 26 BDSG zur Verarbeitung von Beschäftigtendaten gilt nicht nur für die Verarbeitung der Daten der Kanzleibeschäftigten. Diese Rechtsgrundlage kann zudem in der Lohn- und Gehaltsbuchhaltung im Auftrag des Mandanten für die Verarbeitung der Daten der Beschäftigten der Mandanten herangezogen werden; der Anwendungsbereich des § 26 BDSG erstreckt sich auch auf Auftragnehmer oder Dritte, die für den Arbeitgeber personenbezogene Daten im Beschäftigungskontext verarbeiten.[7]

2.1.2 Grundsatz der „Richtigkeit"

Nach dem Grundsatz der Datenrichtigkeit müssen Datensätze auf dem neuesten Stand gehalten werden, unrichtige Daten müssen berichtigt oder gelöscht werden. Im Datenschutz-Leitfaden sollte insbesondere nachvollziehbar dokumentiert werden, wie in Fällen der Geltendmachung von Berichtigungs- und Löschungsansprüchen verfahren wird. Werden Ansprüche seitens Nicht-Mandanten geltend gemacht, muss der Steuerberater vorrangig das Berufsgeheimnis beachten, bevor er Auskünfte an Nicht-Mandanten gibt oder Datensätze ändert oder gar löscht. Mit einer Arbeitsanweisung an die Kanzleiangehörigen ist der verantwortliche Steuerberater zugleich gerüstet, auf tatsächliche oder vermeintliche Ansprüche der betroffenen Personen angemessen und zeitnah zu reagieren.[8]

2.1.3 IT-Sicherheitskonzept nach dem Grundsatz der „Integrität und Vertraulichkeit" und TOM

Hinter dieser Begrifflichkeit steht die Einhaltung der Datensicherheit mittels TOM, die in Art. 32 DSGVO näher ausgestaltet ist. Die Grundsätze und Überlegungen, die zum früheren § 9 BDSG aF nebst Anlage entwickelt wurden, sind trotz des geänderten Wortlauts in Art. 32 DSGVO nach wie vor heranzuziehen.[9] Daher können die bisherigen TOMs zum Schutz personenbezogener Daten zunächst beibehalten werden, sofern sie dem aktuellen Stand der Technik entsprechen und geeignet sind, ein dem Risiko angemessenes Schutzniveau[10] zu erfüllen. Neuerdings dürfen zugunsten des Steuerberaters nach Art. 32 Abs. 1, Hs. 1 DSGVO die „Implementierungskosten" einer Schutzmaßnahme in der Interessenabwägung berücksichtigt werden. Je höher das Risiko für die Rechte und Freiheiten der von der Datenerhebung betroffenen Personen ist, desto höhere Implementierungskosten gelten als zumutbar.[11] Ein unverhältnismäßiger Aufwand darf aber gerade von kleinen und mittelgroßen Steuerberatungskanzleien nicht verlangt werden. Der IT-Leitfaden sollte daher die umsetzbaren und in der täglichen Praxis ausgeführten technischen und organisatorischen Maßnahmen zur Wahrung der IT-Sicherheit beschreiben.

2.2 Anpassung der Einwilligungserklärungen und Datenschutzhinweise

Einwilligungserklärungen sind sowohl nach altem als auch neuem Datenschutzrecht einzuholen, bevor Telefonnummern und E-Mail-Adressen der Kanzleiangehörigen im Internet veröffentlicht, Einträge in Kontaktformulare auf den Kanzleiwebseiten oder zum Bezug eines Newsletters ermöglicht werden etc. Dabei sollte sichergestellt sein, dass die Einwilligungserklärungen beweissicher protokolliert werden.[12] Entsprechend sollten die Datenschutzhinweise mit Informationen zur Verarbeitung personenbezogener Daten auf den Kanzleiwebseiten an die neuen Vorschriften angepasst werden.[13] Inhaltlich müssen Datenschutzhinweise und vorformulierte Einwilligungserklärungen in klarer und einfacher Sprache über Zwecke, Art, Umfang und Dauer der Datenspeicherung informieren. Die Einwilligung muss freiwillig in informierter Weise erklärt werden. Dabei muss über die Möglichkeit des Widerrufs der Einwilligung aufgeklärt werden.

2.3 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten (VVT) ist nicht öffentlich und muss betroffenen Personen nicht offengelegt werden. Es dient der kanzleiinternen Qualitätskontrolle sowie auf Anfrage dem Nachweis gegenüber der Aufsichtsbehörde für den Datenschutz, in welchen Verfahren in welcher Art und Weise mit welchen Kategorien von personenbezogenen Daten umgegangen wird.[14] Steuerberater müssen ein VVT erstellen, schon weil die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt und im Regelfall sensible Daten verarbeitet werden (Art. 9 Abs. 5 DSGVO). Bereits die Konfession des steuerpflichtigen Mandanten ist ein sensibles Datum, da sie Aufschluss über die religiöse Überzeugung des Mandanten bietet. Kanzleien, deren Datenschutzbeauftragte bislang ein Verfahrensverzeichnis nach § 4g Abs. 2 und Abs. 2a BDSG aF geführt haben, können dieses zum Teil übernehmen und an das nunmehr gemäß Art. 30 DSGVO zu führende VVT anpassen. In Art. 30 Abs. 1 DSGVO sind die notwendigen Inhalte des VVT beschrieben. Hierzu gehören die Zwecke der Verarbeitung, eine Beschreibung der personenbezogenen Daten, der betroffenen Personen und Empfänger, die jeder Verarbeitungstätigkeit zugeordnet werden müssen. Die Erstellung des VVT erfordert Aufwand, man gewinnt jedoch einen guten Überblick über die Arbeitsprozesse, in denen personenbezogene Daten verarbeitet werden und ist für Anfragen vorbereitet.[15] Bei der Festlegung der Verarbeitungszwecke darf und sollte der Steuerberater neben den Mandanteninteressen (zB Erfüllung des Mandatsvertrages, Einhaltung übernommener Aufbewahrungsfristen usw) auch die legitimen eigenen Interessen einbeziehen (zB Absicherung von Vergütungsansprüchen, Erhaltung von Verteidigungsmöglichkeiten gegen denkbare Haftungsansprüche in der Gestaltungsberatung usw). Je ausführlicher die rechtmäßigen Zwecke zu einer Verarbeitungstätigkeit dokumentiert sind, desto geringer wird später die Wahrscheinlichkeit sein, dass eine Zweckänderung erforderlich wird, die nur

unter eingeschränkten Voraussetzungen zulässig ist.[16] Daher kann eine sorgfältige Beschreibung der Verarbeitungszwecke im VVT für die späteren Verarbeitungstätigkeiten grundlegend sein.

2.4 Datenschutzbeauftragter

Der verantwortliche Kanzleiinhaber muss prüfen, ob ein Datenschutzbeauftragter (DSB) zu benennen ist. Der Kanzleiinhaber muss jedenfalls immer dann einen DSB benennen, wenn er idR mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Unbedeutend ist dabei, mit welchem Stundenumfang jemand beschäftigt ist (also zählen zB auch Halbtagskräfte als volle Person). Noch nicht geklärt ist die Rechtsfrage, ob bei der Personenzahl die Kanzleiinhaber mitzuzählen sind. Nach der hier unterstützten Auffassung geht aus dem Gesetzeswortlaut „beschäftigen" in § 38 Abs. 1 S. 1 BDSG hervor, dass es nur um die Zahl der Personen geht, die der Kanzleiinhaber beschäftigt, jedoch nicht der Kanzleiinhaber mitzuzählen ist. Der Begriff „Beschäftigte" umfasst gemäß § 28 Abs. 8 BDSG neben Arbeitnehmern zB auch die Auszubildenden, Praktikanten und Leiharbeitnehmer, nicht jedoch den Inhaber einer Kanzlei oder etwa die Gesellschafter einer Steuerberatungs-GmbH.[17] Da es hierzu noch keine gefestigte Meinung gibt, sollte bis zur eindeutigen Klärung dieser offenen Rechtsfrage vorsorglich ein DSB benannt werden, wenn regelmäßig und ständig mindestens zehn Personen einschließlich Kanzleiinhaber bzw. Gesellschafter mit der automatisierten Verarbeitung von personenbezogenen

Daten zu tun haben.

Die in Art. 37 Abs. 1 DSGVO genannten Gründe, die einen DSB unabhängig von der Beschäftigtenzahl erforderlich machen, kommen in Steuerberatungskanzleien eher selten vor. Insbesondere wird die Verarbeitung besonderer Datenkategorien (sensible Daten, zB Gesundheitsdaten und Religionsdaten in der Steuerberatung und Lohnbuchhaltung) nicht als „Kerntätigkeit" iSv Art. 37 Abs. 1 Buchst. c DSGVO angesehen.[18] Auch wird nicht davon ausgegangen, dass in kleinen bzw. mittelständischen Steuerberatungskanzleien mit weniger als zehn Beschäftigten die Verarbeitung von sensiblen Daten im Regelfall umfangreich sei und damit idR keine Pflicht zur Durchführung einer Datenschutzfolgenabschätzung begründet würde.[19]

Die Anforderungen an die Qualifikation und Stellung des DSB ergeben sich aus Art. 37, 38 DSGVO und § 38 BDSG. Er muss über ein angemessenes Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis verfügen, um seine Aufgaben erfüllen zu können, die in Art. 39 DSGVO definiert sind. Der Kanzleiinhaber muss sicherstellen, dass der DSB in Ausübung seiner sonstigen Aufgaben keinem Interessenkonflikt unterliegt. Daher dürfen insbesondere nicht Führungskräfte, wie beispielsweise Leiter der IT-Abteilung, Personalabteilung oder Mitglieder der Geschäftsleitung zum DSB benannt werden.[20]

2.5 Arbeitsanweisung zu Informationspflichten und Betroffenenrechten

Vorweg sollte eines hervorgehoben werden: Der Steuerberater muss zuerst für die Wahrung des Berufsgeheimnisses Sorge tragen, bevor er auf mögliche Betroffenenrechte anfragender Personen eingeht. Um auf Anfragen betroffener Personen in der Praxis angemessen reagieren zu können, ist eine entsprechende Arbeitsanweisung an das Kanzleipersonal zu empfehlen. Die Anweisung legt zB fest, wie Informationspflichten rechtzeitig erfüllt werden, in welcher Form die Identität eines Anfragenden geprüft wird, ob das Berufsgeheimnis der begehrten Auskunftserteilung entgegensteht und in welcher Weise ggf. auf berechtigt geltend gemachte Betroffenenrechte auf Auskunft, Berichtigung, Löschung und „Recht auf Vergessenwerden", Einschränkung der Verarbeitung (Art. 18, 19 DSGVO) sowie auf Datenübertragbarkeit (Art. 20 DSGVO) reagiert werden kann.

Im Rahmen der *Informationspflichten* (Art. 13, 14 DSGVO, §§ 32, 33 BDSG) muss der Steuerberater bei Mandanten oder sonstigen Personen die in Art. 13 Abs. 1 DSGVO dargelegten Informationen zur Datenverarbeitung aufklären.[21] Diese Pflicht besteht bereits im Zeitpunkt der Erhebung von personenbezogenen Daten. Um im ersten Beratungsgespräch hinreichend informieren zu können, empfiehlt es sich, die Datenverarbeitung anhand eines gesonderten Informationsblattes mit dem Mandanten zu besprechen und sich die Kenntnisnahme unterschreiben zu lassen.[22] Aus dem Wortlaut in Art. 13 Abs. 1 DSGVO „teilt der Verantwortliche ... zum Zeitpunkt der Erhebung ... mit" sowie des Gültigkeitszeitpunktes der DSGVO ergibt sich, dass die Informationspflicht nicht für Bestandsdaten gilt, die vor dem 25.5.2018 erhoben wurden. Bei der Erhebung von Daten betroffener Dritter (zB Mitarbeiter des Mandanten) hat der Steuerberater idR keine Pflicht zur Information des Drittbetroffenen, weil das Berufsgeheimnis dem entgegensteht (Art. 14 Abs. 5 Buchst. d DSGVO). Im Einzelfall kann dies anders sein, zB wenn der Mandant den Steuerberater von der Verschwiegenheitspflicht befreit.[23]

Von der Informationspflicht des Steuerberaters unterscheidet sich das *Auskunftsrecht* der betroffenen Person (Art. 15 DSGVO, § 34 BDSG). Diese hat das Recht, die in Art. 15 Abs. 1 DSGVO aufgeführten Informationen anzufragen und zu erfahren. Auch hier besteht bei anfragenden Nicht-Mandanten keine Auskunftsverpflichtung des

Steuerberaters, wenn die Auskunftserteilung gegen das Berufsgeheimnis verstoßen würde (§ 29 Abs. 1 S. 2 BDSG).[24]

Neben dem Recht auf *Berichtigung* unrichtiger personenbezogener Daten (Art. 16 DSGVO) können betroffene Personen ein Recht auf Löschung (sog. Recht auf Vergessenwerden) haben (Art. 17 DSGVO, § 35 BDSG). Bevor personenbezogene Daten unwiederbringlich gelöscht werden, sollte die Arbeitsanweisung eine sorgfältige Prüfung vorsehen, ob ein Löschungsgrund[25] nach Art. 17 Abs. 1 DSGVO vorliegt und ob der Löschungsanspruch nicht gemäß Art. 17 Abs. 3 DSGVO ausgeschlossen ist. In der Praxis können zB offene Vergütungsansprüche oder die zukünftige Absicherung gegen mögliche Haftungsforderungen gegen den Steuerberater einen Löschungsanspruch des Mandanten ausschließen (Art. 17 Abs. 3 Buchst. e DSGVO). Auch die Verpflichtung zur Aufbewahrung der Handakte kann gemäß Art. 17 Abs. 3 Buchst. b DSGVO gegen einen Löschungsanspruch herangezogen werden, soweit und solange der Steuerberater dieser Aufbewahrungsverpflichtung gemäß § 66 StBerG unterliegt.

2.6 Regelungen zur Auftragsverarbeitung

Einige Datenschutzbeauftragte von Mandanten verlangen den Abschluss von Auftragsverarbeitungsverträgen mit Steuerberatern im Rahmen des steuerlichen Mandatsverhältnisses. Dem ist Folgendes entgegenzuhalten: Der Steuerberater ist nicht Auftragsverarbeiter des Mandanten, da er keine Unterstützungshandlungen bei der Datenverarbeitung, sondern Dienstleistungen eigener Art erbringt.[26] Dies sind eigenverantwortliche Fachleistungen im Rahmen der Steuerberatertätigkeit nach dem StBerG. Demzufolge brauchen Steuerberater und die sonstigen in § 3 StBerG genannten Berufsgruppen keine Auftragsverarbeitungsverträge iSv Art. 28 DSGVO mit ihren Mandanten abzuschließen, wenn sie Leistungen nach dem StBerG erbringen. Dazu gehören auch die Leistungen im Rahmen der Lohn-, Gehalts- und Finanzbuchführung. Die steuerberatenden Tätigkeiten müssen nach § 57 Abs. 1 StBerG ua unabhängig und eigenverantwortlich erbracht werden. Demgegenüber darf die Auftragsverarbeitung nach Art. 29 DSGVO „ausschließlich auf Weisung" des Auftraggebers ausgeführt werden. Das ist mit der eigenverantwortlichen Fachleistung der steuerberatenden Berufe nicht vereinbar. Nach dem Kurzpapier Nr. 13 der Datenschutzkonferenz, dem die Aufsichtsbehörden für den Datenschutz des Bundes und der Länder angehören, sind die Arbeiten der Steuerberater wie auch der anderen Berufsgeheimnisträger „fremde Fachleistungen", die eigenverantwortlich erbracht werden und somit keine weisungsabhängige Auftragsverarbeitung.[27] Die Meinungsbildung ist jedoch in diesem Punkt zur Lohn-, Gehalts- und Finanzbuchführung noch nicht abgeschlossen. Die Behördenpraxis und Rechtsprechung müssen zu dieser Frage weiter beobachtet werden. Sofern demgegenüber Rechenzentren ausschließlich automatisierte DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchführung ohne jegliche Beratungsleistung erbringen, ist dies als Auftragsverarbeitung zu qualifizieren.[28] Hiervon unterscheidet sich die Tätigkeit des Steuerberaters als Berufsgeheimnisträger zur Lohn-, Gehalts- und Finanzbuchführung, bei der die eigenverantwortliche, unabhängige und verschwiegene Berufsausübung im Vordergrund steht.

In der Kanzleiorganisation ist sicherzustellen, dass die Auftragsverarbeitungsverträge mit den

externen Dienstleistern der Kanzlei (zB Anbieter der Kanzleisoftware, externe IT-Administratoren, Aktenvernichter) dem aktuellen Stand entsprechen. Mit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen v. 30.10.2017[29] wurden die Rechtsunsicherheiten beseitigt, die bislang mit dem Outsourcing an Dienstleister verbunden waren, die nicht dem Berufsgeheimnis unterliegen. Nunmehr unterfällt das Offenbaren von geschützten Geheimnissen an Personen, die an der beruflichen Tätigkeit des Berufsgeheimnisträgers mitwirken (externe Dienstleister), nicht mehr der Strafbarkeit des § 203 StGB, soweit dies für die ordnungsgemäße Durchführung der Tätigkeit der mitwirkenden Personen erforderlich ist (§ 203 Abs. 3 S. 2 StGB). Die konkreten Anforderungen, die an den Dienstleister eines Steuerberaters zu stellen sind, ergeben sich aus dem neu eingefügten § 62a StBerG.[30] Für die Praxis macht die neue Rechtslage eine Ergänzung der Auftragsverarbeitungsverträge oder eine separate Vereinbarung erforderlich, um die neuen Anforderungen des § 62a StBerG zu erfüllen.[31] Zum Teil haben die Softwaredienstleister bereits eine entsprechende Vereinbarung in ihre Auftragsverarbeitungsverträge integriert.

2.7 Meldeverfahren für Datenpannen

Datenschutzverletzungen müssen grundsätzlich mit den in Art. 33 Abs. 3 DSGVO vorgegebenen Informationen innerhalb von 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde für den Datenschutz gemeldet werden. Das gilt nur dann nicht, wenn der Steuerberater darlegen kann, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Die kurze Frist macht eine sofortige Risikoprognose oder alternativ eine vorsorgliche Meldung der Datenpanne erforderlich. Eine Meldung ist dann nicht erforderlich, wenn die Prognose nach Eintrittswahrscheinlichkeit und Schadenshöhe nur ein geringfügiges Risiko ergibt, bei dem eine Meldung nach Abwägung der Gefahrenaspekte nicht erforderlich erscheint.[32] Zur Vorbereitung auf eine jederzeit mögli-

che Datenpanne sollte sich die Kanzleileitung frühzeitig mit den Meldeverfahren auf den Webseiten der zuständigen Aufsichtsbehörde für den Datenschutz (idR Beauftragte/r des jeweiligen Bundeslandes für den Datenschutz und die Informationsfreiheit) auseinandersetzen. Im Zweifel reicht eine formlose aber dokumentierte Meldung an die Aufsichtsbehörde mit den in Art. 33 Abs. 3 DSGVO beschriebenen Inhalten.

Ergibt die Prognose ein voraussichtlich hohes Risiko, müssen nach Art. 34 DSGVO zudem die betroffenen Personen in einfacher und klarer Sprache mit den gleichen Inhalten wie nach Art. 33 Abs. 3 DSGVO unverzüglich von der Datenpanne informiert werden. Eine Information an die betroffenen Personen ist nach Art. 34 Abs. 3 DSGVO ausnahmsweise dann nicht erforderlich, wenn die Daten durch geeignete Methoden unzugänglich gemacht worden sind. Daher sollten zB mobile Datenträger ausreichend sicher verschlüsselt werden, um die Daten der betroffenen Personen in Fällen des Datenträgerverlustes ausreichend zu schützen.[33]

2.8 Aufbewahrungs- und Löschkonzept

Bei vielen Steuerberatern besteht die Neigung, Akten für relativ lange Zeiträume oder gar

unbefristet aufzubewahren. Anfragen von Mandanten können es auch noch lange Zeit nach Ablauf der gesetzlichen Aufbewahrungsfristen erforderlich machen, Dokumente aus den archivierten Akten hervorzuholen. Das legitime Interesse an einer möglichst langfristigen Aufbewahrung muss mit dem Grundsatz der (zeitlichen) „Speicherbegrenzung" nach Art. 5 Abs. 1 Buchst. e DS-GVO in Einklang gebracht werden. Danach dürfen personenbezogene Daten grundsätzlich nur so lange aufbewahrt werden, wie es ihr Verarbeitungszweck erfordert. Auch unter diesem Gesichtspunkt ist eine sorgfältige Dokumentation der Verarbeitungszwecke und vorgesehenen Löschfristen wichtig.

Aufbewahrungsfristen ergeben sich aus dem Steuer- und dem Handelsrecht. Handelsrechtliche Aufbewahrungspflichten von Unternehmen werden idR vom Steuerberater im Mandatsverhältnis übernommen und stellvertretend erfüllt. Für Handakten iSv § 66 StBerG ergibt sich grundsätzlich eine Aufbewahrungsfrist von zehn Jahren nach Auftragsbeendigung. Unterlagen, die für die Besteuerung relevant sind, müssen ggf. über zehn Jahre hinausgehend aufbewahrt werden, wenn die Festsetzungsfrist noch nicht abgelaufen ist. Die BStBK vertritt die Auffassung, dass zur zehnjährigen Aufbewahrungsfrist ein pauschaler Zuschlag von weiteren vier Jahren zulässig und empfehlenswert ist, um auch eine mögliche Ablaufhemmung einzuschließen.[34] Hieraus ergibt sich eine Aufbewahrungsfrist von 14 Jahren, nach deren Ablauf im Einzelfall zu prüfen ist, ob legitime Gründe für eine weitere Aufbewahrung vorliegen. Um ein praktikables und sicheres Löschverfahren zu ermöglichen und versehentliche Löschungen zu vermeiden, ist nach Meinung der BStBK eine weitere Karenzzeit von sechs Monaten angemessen, bis die Dateien unwiederbringlich gelöscht werden.[35] Die Vorgehensweisen zur Löschung personenbezogener Daten müssen von der Kanzlei in einem Löschkonzept dokumentiert werden. Dies ergibt sich aus der „Rechenschaftspflicht" gemäß Art. 5 Abs. 2 iVm Abs. 1 Buchst. e DSGVO.[36] Seitens der Aufsichtsbehörden liegen jedoch noch keine Aussagen zur zulässigen Aufbewahrungsdauer und Praxis der Löschkonzepte der Steuerberater vor. Die Behördenpraxis und Rechtsprechung müssen daher verfolgt werden, um ggf. die Löschkonzepte entsprechend anzupassen.

3. Fazit und Ausblick

Sowohl der Berufsstand der Steuerberater als auch die Aufsichtsbehörden für den Datenschutz stehen noch am Anfang der praktischen Umsetzung des neuen EU-Datenschutzrechts. Im Zuge des digitalen Wandels wachsen die Gefahren für die personenbezogenen Daten von Mandanten, Beschäftigten und anderen betroffenen Personen. Damit besteht ohne Zweifel die Notwendigkeit zur Einrichtung eines modernen Datenschutzmanagements in der Steuerberatungskanzlei. Dieses kann sich in der Zukunft zu einem Qualitätsmerkmal in der Steuerberatung entwickeln. Zugleich dürfen dabei die formalen Anforderungen an die Konzeption und Dokumentation der durchzuführenden Maßnahmen in der Kanzleiorganisation nicht zu einem unverhältnismäßigen Aufwand führen. Die Berufsorganisationen verfolgen daher den Ansatz, in Zusammenarbeit mit den Aufsichtsbehörden praktikable Lösungen zu finden, die sowohl den Schutz der Rechte und Freiheiten der von der Datenerhebung betroffenen Personen wahren, als auch das berechtigte Anliegen der Steuerberater, sich in der alltäglichen Arbeit nicht auf den Datenschutz, sondern auf das Kerngeschäft konzentrieren zu können: die Beratung der Mandanten in ihren steuerlichen und wirtschaftlichen Angelegenheiten.

---

* *Roland Kleemann*, StB/WP/RA, ist Präsident der Steuerberaterkammer Berlin und Mitglied des Präsidiums der BStBK, *Martin Kader*, RA, ist Referent der Steuerabteilung der BStBK.

1 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). Mit einem zweiten DSAnpUG-EU ist dem Vernehmen nach in der zweiten Jahreshälfte 2018 zu rechnen.

2 Vgl. *Laue* ZD 2016, 463 (464 f.).

3 „Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften" des gemeinsamen Arbeitskreises der BStBK und des DStV e.V., abrufbar unter: www.bstbk.de/Presse/Publikationen/Fachinfos.

4 Die übrigen in Art. 5 Abs. 1 DSGVO genannten Verarbeitungsgrundsätze sind ohnehin im Verzeichnis der Verarbeitungstätigkeiten (Verarbeitung nach „Treu und Glauben", „Transparenz", „Zweckbindung" und „Datenminimierung") bzw. im Aufbewahrungs- und Löschkonzept („Speicherbegrenzung") zu dokumentieren. Der Aufwand für den Datenschutz-Leitfaden kann daher gering gehalten werden.

5 Vgl. Kurzpapier Nr. 17 der Datenschutzkonferenz (DSK) v. 27.3.2018, 1 f., abrufbar zB unter dem Link: https://www.lda.bayern.de/media /dsk_kpnr_17_besondere_kategorien.pdf.

6 Vgl. Kurzpapier Nr. 17 (Fn. 5).

7 *Wybitul* NZA 2017, 413 (414); *Gräber/Nolden* in Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, BDSG § 26 Rn. 6.

8 S. im Einzelnen zu den Betroffenenrechten die „Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften" der BStBK und des DStV e.V., Ziff. 9.3–9.9.

9 *Paulus* in Wolff/Brink, BeckOK Datenschutzrecht, Stand: 1.2.2017, DS-GVO Art. 32 Rn. 6.

10 Vgl. die weiterführenden Hinweise von *Martini* in Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 46–60.

11 *Jandt* in Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Rn. 11.

12 Zum Double-Opt-In-Verfahren im Online-Marketing s. *Munker* in DWS-Merkblatt Nr. 1815, Datenschutz in der Steuerberatungskanzlei, Stand März 2018, 3.

13 Vgl. Muster der BStBK und des DStV e.V. für eine Datenschutzerklärung für die Kanzleiwebsite; DWS-Vordruck Nr. 1008, Datenschutzerklärung für die Website von Steuerberatern (in Vorbereitung).

14 Vgl. *Ehmann/Kranig*, Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, 2017, 12.

15 Vgl. Muster zum VVT des gemeinsamen Arbeitskreises der BStBK und des DStV e.V., abrufbar unter dem Link: https://www.bstbk.de/de/presse/news/2018-04- -05_Praxishilfen_Datenschutz/index.html.

16 Vgl. Art. 6 Abs. 4 DSGVO, § 24 BDSG.

17 Die hier vertretene Auffassung wurde zum früheren § 4f Abs. 1 S. 4 BDSG aF (der ebenfalls in seinem Wortlaut von „beschäftigen" sprach) zB vertreten von *Gola/Klug* NJW 2007, 118 (120).

18 Vgl. Hinweise der BStBK und des DStV e.V. (Fn. 8), Ziff. 10.2.1.

19 Vgl. dazu Bayerisches Landesamt für Datenschutzaufsicht, Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine etc, Muster 4: Steuerberater, abrufbar unter: https://www.lda.bayern.de/media /muster_4_steuerberater.pdf.

20 *Heberlein* in Ehmann/Selmayr, EU-DSGVO, 2017, Art. 38 Rn. 21, 22.

21 Vgl. Hinweise der BStBK und des DStV e.V. (Fn. 8), Ziff. 9.1.

22 Vgl. DWS-Vordruck Nr. 1005, Datenschutzinformation für Mandanten.

23 Vgl. *Backu* DStR 2017, 2699 (2701); Hinweise der BStBK und des DStV e.V., (Fn. 8), mit Verfahrensdokumentation zur Erfüllung der Informationspflichten in Ziff. 9.1.4.

24 Vgl. die Hinweise der BStBK und des DStV e.V., (Fn. 8), mit Verfahrensdokumentation zur Erfüllung der Auskunftspflichten in Ziff. 9.4.3.

25 Vgl. zu den Löschungsgründen im Einzelnen *Paal* in Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, DSGVO Art. 17 Rn. 22–28.

26 Vgl. *Klug* in Gola, Datenschutz-Grundverordnung, 2017, Art. 28 Rn. 5.

27 Vgl. Kurzpapier Nr. 13 der Datenschutzkonferenz (DSK), Auftragsverarbeitung, Stand 16.1.2018, DS-GVO Art. 28, 4 Anhang B.

28 Vgl. Kurzpapier Nr. 13 (Fn. 27), 4 Anhang A.

29 BGBl. I 2017, 3618–3624.

30 Vgl. *Brüggemann/Rein* DStR 2017, 2572 (2574); *Backu* DStR 2017, 2699.
31 Vgl. das Muster „Zusatzvereinbarung zum Auftragsverarbeitungsvertrag" in den Hinweisen der BStBK und des DStV e.V., (Fn. 8), Ziff. 7.1.3.
32 *Martini* (Fn. 10), DS-GVO Art. 33 Rn. 22–26.
33 Vgl. zu den Verschlüsselungsmethoden die Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI): www.bsi-fuer-buerger.de (> Empfehlungen > Verschlüsselung).
34 Hinweise der BStBK und des DStV e.V. (Fn. 8), Ziff. 13.
35 Hinweise der BStBK und des DStV e.V. (Fn. 8), Ziff. 13.
36 Vgl. Erwägungsgrund Nr. 39 S. 10 zur DSGVO; *Herbst* in Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 Rn. 67.