Newsletter 06|27.03.2018

Datenschutz-Grundverordnung der EU (DSGVO): Handlungsempfehlungen für Steuerberaterkanzleien

keyboard_arrow_down

Der Countdown zur Umsetzung der DSGVO tickt unerbittlich, denn der 25.05.2018 als Umsetzungsstichtag rückt immer näher. Ab diesem Stichtag müssen datenverarbeitende Unternehmen in der EU die Vorgaben der DSGVO beachten. Und welches Unternehmen oder welcher Mandant verarbeitet keine elektronischen Daten? Die zahlreichen Änderungen des neuen Datenschutzrechts sind mit deutlich erhöhten organisatorischen Anforderungen (Rechenschafts- und Dokumentationspflichten), Bußgeldern und Haftungsrisiken verbunden. Eine aktuelle und repräsentative Umfrage unter Unternehmen der Informationswirtschaft durch das Zentrum für Europäische Wirtschaftsforschung (ZEW) zeigt, dass mehr als die Hälfte der Unternehmen der Informationswirtschaft sich noch gar nicht mit der DSGVO auseinander-gesetzt haben. Die Unternehmen, die das bereits getan haben, sagen, dass es sich um tief- oder sehr tiefgreifende Änderungen handelt. Die Unternehmen nehmen die DSGVO haupt¬sächlich als zusätzliche Kosten- und Arbeitsbelastung wahr und fürchten eine Verkomplizierung der Geschäftsprozesse.
11.
Auch der Berufsstand steht – zusätzlich zur Beachtung der seit dem 26.06.2017 geltenden Neuregelung des Geldwäschegesetzes – vor einer weiteren Herausforderung, die internen Geschäftsprozesse und den Umgang mit personenbezogenen Daten an die Anforderungen des neuen Rechts anzupassen.

Ist der Steuerberater Auftragsverarbeiter?

Wenn personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet werden, liegt eine Auftragsverarbeitung vor, Artikel 4 Nr. 8, 28, 29 DSGVO. Die Anforderungen an die Auftragsverarbeitung wurden im Verhältnis zur DS-RL erheblich verschärft. Ähnlich wie bereits unter § 11 BDSG erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der
personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Durch eine vorgesehene gemeinsame Haftung von Verantwortlichen und Auftragsverarbeitern wird sich das Risiko für die Auftragsverarbeiter erheblich erhöhen. Ob der Steuerberater im Verhältnis zum Mandanten (z. B. im Lohnbuchführungsmandat) Aufragsverarbeiter ist, ist unklar, nachdem der Begriff der Funktionsübertragung nicht in die DSGVO übernommen wurde. Nach h. M. ist der Steuerberater im Verhältnis zum Mandanten kein Auftragsverarbeiter (Berufsrechtliches Handbuch
5.2.4. I, 4.). Einige Datenschutzbeauftragte sind aber der Auffassung, Steuerberater müssen mit ihren Mandanten ab dem 25.05.2018 Auftragsverarbeitungsverträge schließen. Dem kann allerdings die Rechtsauffassung des BMI entgegengehalten werden. Das BMI ist der Auffassung, dass Steuerberater wegen ihrer besonderen Stellung im Regelfall als

Verantwortliche und nicht als Auftragsverarbeiter anzusehen sind. Es sei auch nicht erkennbar, dass sich dies ab dem 25.05.2018 ändern würde, wenn die neuen Vorschriften der DSGVO zur Anwendung kommen. Diese Rechtsauffassung wurde der Bundessteuerberaterkammer
mit Schreiben des BMF vom 21.12.2017 mitgeteilt.
Es besteht deshalb derzeit keine zwingende Notwendigkeit, mit den Mandanten Auftragsverarbeitungsverträge abzuschließen. Verträge mit Auftragsverarbeitern (z.B. Rechenzentren) müssen allerdings bis zum 25.05.2018 an die DSGVO angepasst werden.

Umsetzung der neuen Informationspflichten

Allerdings sieht die DSGVO weitreichende Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen vor (Artikel 13 ff. DSGVO). Es sollen alle Informationen zur Verfügung gestellt werden, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Die Informationen sind der betroffenen Person (z. B. Mandant, Mitarbeiter, Bewerber, etc.), deren Daten verarbeitet werden, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erteilen. Die Übermittlung der Informationen muss grundsätzlich schriftlich erfolgen. Gegenüber Mandanten kann dies auf einem entsprechenden Informationsblatt geschehen. Einfacher ist es, diese Informationen zum Gegenstand der allgemeinen Geschäftsbedingungen zu machen. Der DWS-Verlag hat bereits angekündigt, sämtliche Informationen, die nach Artikel 13 DSGVO gegenüber Mandanten zu erteilen sind in die AGB einzuarbeiten. Mit Verwendung der aktuellen AGB dürften Steuerberater zumindest hinsichtlich der Informationspflichten gegenüber ihren Mandanten gut aufgestellt sein. Gleiches gilt für die vom DWS-Verlag herausgegebenen Steuerberatungsverträge, da die AGB dort bereits integriert sind.

Hinweis: Hinweise zur Verwendung der Steuerberatungsverträge und der AGB des DWS-Verlags finden Sie auf der Internetseite www.dws-verlag.de unter dem Suchbegriff „1001.1“.

Bestellung eines Datenschutzbeauftragten

Die Bestellung eines Datenschutzbeauftragten – intern oder extern – ist für alle Kanzleien verpflichtend, in denen mehr als neun Mitarbeiter ständig personenbezogene Daten verarbeiten. Hierbei sind alle Köpfe zu zählen, einschließlich der Geschäftsleitung (Berufsrechtliches Handbuch 5.2.4. I, 3.). Angesichts der hohen Anforderungen, die an die Person des Daten¬schutz-beauftragten zu stellen sind und angesichts seiner arbeitsrechtlichen Sonderstellung, fragen viele Kollegen nach geeigneten externen Datenschutzbeauftragten. Die Steuerberaterkammer Düsseldorf kann hier keine Empfehlungen aussprechen. (Zertifizierte) Anbieter sind im Internet allerdings schnell gefunden. Gleiches gilt für die Anbieter von Software zur Erstellung eines Verarbeitungsverzeichnisses, das Grundlage für die Umsetzung des Datenschutzes in der Kanzlei ist.

Verarbeitungsverzeichnis

Darin wird jedes einzelne Verfahren in der Kanzlei erfasst, in dem personenbezogene Daten verarbeitet werden. Das sog. „Verzeichnis der Verarbeitungstätigkeiten“ (Verarbeitungsverzeichnis) nach Artikel 30 DSGVO liegt in der Verantwortung der Unternehmensleitung. Die Erstellung dieses Verzeichnisses kann deshalb nicht an den Datenschutzbeauftragten delegiert werden. Informationen zum Inhalt des Verarbeitungsverzeichnisses sowie zu mehreren Anbietern von Software zur Erstellung des Verarbeitungsverzeichnisses finden sich auf
der Internetseite der Bitkom (www.bitkom.org).

Kanzlei-Website und Datenschutzerklärung

Kanzleien mit eigener Website sind mit Inkrafttreten der DSGVO einem Abmahnrisiko ausgesetzt, das es zu vermeiden gilt. Da die Datenschutzkonformität der Kanzlei-Website nach außen für jedermann sichtbar ist, ist mit Abmahnungen durch spezialisierte Rechtsan¬walts-kanzleien zu rechnen. Spätestens ab dem 25.05.2018 sollte der Internetauftritt deshalb über einen Datenschutzhinweis und ein Impressum verfügen, das auch den neuen Anforderungen an die DSGVO genügt. Dazu gehört u. a., dass der Datenschutzhinweis und das Impressum
von jeder Seite des Internetauftritts aus leicht zu erreichen sind. Befinden sich auf der Website Formulare, mit deren Hilfe Daten in die Kanzlei übertragen werden können (Kontaktformulare etc.), ist darauf zu achten, dass die Pflichtangaben sich auf das tatsächlich Notwendige beschränken und ein Hinweis auf die Datenverarbeitung im Datenschutzhinweis erfolgt. Falls die Kanzlei einen Newsletter eingebunden hat, muss die Anmeldung im sog. Double-Opt-In-Verfahren abgebildet werden (doppelte Bestätigung einer Anmeldung über Online-Formulare und E-Mails). Der Einsatz von Tracking-Tools wie Google-Analytics oder Piwik ist nur erlaubt, wenn die Verarbeitung der Daten den Vorschriften des BDSG und TMG entsprechend abgebildet werden kann.

Hinweis: Die Bundessteuerberaterkammer hat die Herausgabe eines Musters für eine solche Datenschutzerklärung angekündigt. Sobald dieses Muster freigegeben ist, werden wir es auf der
Homepage im mitgliedergeschützten Bereich veröffentlichen.

Wer hinsichtlich der Datenschutzerklärung (und der Impressumspflichten) auf der sicheren Seite sein möchte, sollte sich nicht auf die Prüfung durch seinen Internet-Dienstleister verlassen, sondern einen möglichst spezialisierten (Internet-)Rechtsanwalt beauftragen.

Besondere Hilfestellungen für den Berufsstand

BStBK und DStV haben im letzten Jahr eine Arbeitsgruppe gebildet, die sich zur Aufgabe gemacht hat, die Berufsangehörigen bei der Umsetzung der neuen Datenschutzanforderungen praxisgerecht zu unterstützen und Praxishilfen zu erstellen. Sobald diese vorliegen,
werden wir sie im mitgliedergeschützten Bereich auf der Homepage einstellen.

Die StBK Hessen plant Seminarveranstaltungen zur DGSVO im Mai und Juni 2018 in Kassel, Frankfurt am Main und Darmstadt. Hierüber werden wir demnächst in unserem

Kammerrundschreiben und auf unserer Homepage berichten.

Quelle: Kammermitteilung 132 der Steuerberaterkammer Düsseldorf vom 16.03.2018

Fragen und Antworten zu Cloud-Computing und Verschwiegenheitspflicht

keyboard_arrow_down

Fragen:

1. Aufgrund der Umstellung meiner Arbeitsweise würde ich gerne von Ihnen wissen, ob die Nutzung einer Cloud als Ablageort für Notizen zulässig ist oder ob die Verschwiegenheitspflicht dem entgegensteht.
Ich möchte gerne Microsoft OneNote nutzen. Dies ist ein Programm, mit dem man digital Notizen erstellen kann. Das Programm synchronisiert die erstellten Notizen mit der Cloud bei Microsoft namens OneDrive (Server in den USA). Durch die Synchronisation kann ich überall auf meine Notizen zugreifen, also z. B. über mein Smartphone, über mein Tablet oder über den PC im Büro. Je nach Programmversion gibt es aber keine lokale Speicherung der Notizen, sondern nur in der Cloud. Dies ist insbesondere bei der Version für Tablet und Smartphone der Fall.
Wenn ich mandantenbezogene Notizen erstelle, also z. B. mit dem Tablet in einer Besprechung Einzelheiten eines Falles aufnehme (z. B. Name, Geburtstag, Einkommen, Angriffs-/Verteidigungsmittel etc.), kann dies dann mit meiner Verschwiegenheitspflicht kollidieren.

2. Ich bin gerade dabei, meine EDV-Struktur zu verbessern und muss in diesem Zuge auch meinen Exchange Server für den Mailverkehr erneuern. Mein EDV-Partner hat mir zwei Angebote vorgelegt. Klassisch aber teuer wäre die Installation eines Exchange-Servers bei mir in der Kanzlei. Alternativ und kostengünstig wäre das Microsoft Office 365 Business Premium mit einem Hosted Exchange Server. Die Daten befinden sich dann grundsätzlich in einem Rechenzentrum innerhalb der EU. Gegen Aufpreis kann auch ein deutsches Rechenzentrum in Anspruch genommen werden. Darf ich meinen Mail-Server auslagern? Muss ich meine Mandanten darauf hinweisen? Gibt es hier berufsrechtliche Regelungen?

3. Wir überlegen, ob wir zukünftig unsere Mandantenrundschreiben/Newsletter durch einen Dritten direkt an unsere Mandanten verschicken lassen. Hierzu müssten wir dem Auftragnehmer die E-Mail-Adressen und Anreden der Mandanten nennen. Dieser würde dann die Rundschreiben personalisiert (z. B. „Sehr geehrter Herr Müller“) an unsere Mandanten verschicken. Selbstverständlich wird der Auftragnehmer von unserer Seite zur Verschwiegenheitspflicht bezüglich der Mandantendaten verpflichtet. Spricht aus berufsrechtlicher Sicht etwas gegen diese Handhabung?

Antworten:

zu 1: Bei der Beantwortung der Frage sind verschiedene Aspekte zu beachten: das Strafrecht, das Berufsrecht und das Datenschutzrecht.

Neue Straftatbestände für Steuerberater und externe Dienstleister

Bekanntlich können Steuerberater sich wegen der Verletzung von Privatgeheimnissen strafbar machen, wenn sie unbefugt ein fremdes Geheimnis offenbaren, dass ihnen als Steuerberater anvertraut oder bekannt geworden ist, § 203 Abs. 1 Nr. 3 StGB. Die Vorschrift wurde durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen erweitert und ermöglicht u.a. Steuerberatern nunmehr unter näher geregelten Voraussetzungen das Outsourcing von Dienstleistungen. Neben den traditionellen Dienstleistungen Dritter (z. B. externe Aktenlagerung oder -entsorgung, Empfangs- und Sicherheitsdienste, externe Telefonzentralen und Sekretariate etc.) ist damit in erster Linie das klassische IT-Outsourcing in Form des Cloud Computing gemeint. Der Gesetzgeber hat eine eigene Strafbarkeit des externen Dienstleisters in § 203 Abs. 4 S. 1 StGB begründet, wenn dieser unbefugt ein fremdes Geheimnis offenbart, das ihm bei Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt geworden ist. Bestraft wird aber auch der Steuerberater, der nicht dafür Sorge trägt, dass der externe Dienstleister zur Geheimhaltung verpflichtet wird, § 203 Abs. 4 S. 2 Nr. 1 StGB.

Vertrag mit externem Dienstleister zwingend vorgeschrieben

Die neuen strafrechtlichen Regelungen werden flankiert durch einen erweiterten § 62 StBerG (Verschwiegenheitspflicht beschäftigter Personen) und einen neuen § 62a StBerG (Inanspruchnahme von Dienstleistungen). Danach sind Steuerberater nunmehr verpflichtet, mit dem Dienstleister einen Vertrag in Textform zu schließen und diesen unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten. In dem Vertrag muss auch festgelegt werden, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrages heranzuziehen. Für diesen Fall ist ihm aufzuerlegen, diese Personen ebenfalls in Textform zur Verschwiegenheit zu verpflichten, § 62a Abs. 3 StBerG. Dies bedeutet, dass sich der externe Dienstleister bewusst dafür entscheiden muss, ein eigenes Strafbarkeitsrisiko zu übernehmen. Der Steuerberater als Geheimnisverpflichteter muss versuchen, bei seinem Vertragspartner ein entsprechendes Bewusstsein dafür zu schaffen.

Sorgfältige Auswahl des Dienstleisters

Der Steuerberater ist verpflichtet, den Dienstleister sorgfältig auszuwählen, § 62a Abs. 2 S. 1 StBerG. Die Regelung korrespondiert mit den Artikeln 24, 25, 32, 35 und 36 der Datenschutzgrundverordnung (DSGVO), die am 25.05.2018 in Kraft tritt. Danach besteht eine Dokumentationspflicht im Hinblick auf die Auswahl der externen Dienstleister unter Berücksichtigung von Risikobewertungen. In diesem Zusammenhang ist es von Vorteil, wenn der externe Dienstleister zertifiziert ist. Die Firma Microsoft widmet sich auf ihren Internetseiten intensiv dem Thema Datenschutz und DSGVO. Sie weist dort u.a. ausdrücklich darauf hin, dass eigens entwickelte Werkzeuge für die Erfüllung der DSGVO-Anforderungen auch bei Cloud-Diensten von Microsoft sorgen. Auf den ersten Blick scheinen damit die Anforderungen an die sorgfältige Auswahl des externen Dienstleisters erfüllt zu sein.

Insbesondere ergibt sich aus den o. g. gesetzlichen Regelungen keine Verpflichtung, ggf. sicherere Alternativen zu der Web-Speicherlösung von Microsoft-OneDrive oder anderen vergleichbaren Anbietern (z. B. iCloud, Dropbox, Google-Drive, WeTransfer) auszuwählen.

Problem: Server-Standort USA

Problematisch ist allerdings Ihr Hinweis auf den Server-Standort in den USA. Gemäß § 62a Abs. 4 StBerG darf der Steuerberater bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, den Dienstleister nur dann beauftragen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Da der Steuerberater dies nicht in jedem Fall verlässlich beurteilen kann, ist er nur dann auf der sicheren Seite, wenn er zuvor die Einwilligung aller betroffenen Mandanten eingeholt hat. Dieses praktische Problem stellt sich nicht, wenn der Speicherort nicht in den USA, sondern in Deutschland ist. Obwohl die am häufigsten genutzten Cloud-Anwendungen fast alle aus den USA stammen, haben viele amerikanische Anbieter zwischenzeitlich Rechenzentren in Europa und Deutschland eingerichtet und erklären sich bereit, die Datenspeicherung auf diese Orte (gegebenenfalls gegen höhere Gebühren) zu beschränken. Dabei ist im Einzelfall zu klären, ob dies nur den Speicherort betrifft oder auch den Support durch Wartungspersonal. Ein Verstoß gegen § 62a Abs. 4 StBerG ist im Übrigen „nur“ von berufsrechtlicher und nicht von strafrechtlicher Relevanz, da § 203 StGB eine Einschränkung bei ausländischen Anbietern nicht vorsieht.

Zu 2: Die Beantwortung dieser Frage ergibt sich im Wesentlichen schon aus der Beantwortung der ersten Frage. Bei der Verwendung eines Exchange-Kontos werden Ihre E-Mail-Nachrichten an Ihr Postfach auf dem Exchange-Server gesendet und in diesem gespeichert. Gleiches gilt für Ihre Kontakte und Ihren Kalender. Da davon auszugehen ist, dass die Firma Microsoft die datenschutzrechtlichen Anforderungen nach der DSGVO erfüllt (s. o. 1) und die Daten auf einem Server innerhalb der EU gespeichert werden, bedarf es lediglich eines Vertrages in Textform mit den Inhalten des § 62a Abs. 3 StBerG (s. o. 1). Allerdings sollte auch hier die Frage des Zugriffs auf die Daten durch Support und Wartungspersonal mit dem Anbieter geklärt werden, da der Server-Standort keine Gewähr dafür bietet, dass nicht doch aus dem amerikanischen Ausland auf die Daten zugegriffen wird.

Zu 3: Sowohl nach § 203 Abs. 3 S. 2 StGB als auch nach § 62a Abs. 1 S. 1 StBerG ist die Offenbarung von Geheimnissen nur zulässig, soweit dies für die Inanspruchnahme der Tätigkeit der Dienstleistung erforderlich ist. Der Steuerberater muss also in jedem Einzelfall prüfen, ob und inwieweit eine Offenbarung bzw. Kenntnisnahmemöglichkeit von geschützten Daten (hier: E-Mail-Adresse und Nachname) durch den externen Dienstleister erforderlich ist. Wenn es gleich geeignete und weniger eingreifende Möglichkeiten gibt, fehlt es möglicherweise an der Erforderlichkeit der Offenbarung. Der Versand von Mandantenrundschreiben und Newsletter könnte auch so organisiert werden, dass der Versand aus der eigenen Kanzlei erfolgt. In diesem Fall wäre ein Offenbaren der E-Mail-Adressen der Mandanten und deren Namen gegenüber einem externen Dienstleister nicht erforderlich. Aus diesem Grunde empfiehlt es sich, die Einwilligung der Mandanten einzuholen, dass diese in Form eines Mandantenrundschreibens/Newsletters (ggf. durch einen externen Dienstleister) informiert werden möchten. Wird das Einverständnis erteilt, bestehen keine Bedenken, einen externen Dienstleister zu beauftragen, wenn dieser

vertraglich gemäß § 62a StBerG verpflichtet wird (s.o. 1 und 2).

Im Vorgriff auf die am 25.05.2018 in Kraft tretende Datenschutzgrundverordnung sollte die Einwilligung zum Newsletter-Bezug datenschutzkonform ausgestaltet werden (Double-Opt-In-Verfahren). Bei diesem Verfahren muss die Eintragung in eine Newsletter-Abonnentenliste in einem zweiten Schritt bestätigt werden. Hierzu wird in der Regel eine E-Mail-Nachricht mit der Bitte um Bestätigung an die eingetragene E-Mail-Adresse versandt. Die Registrierung erfolgt erst dann, wenn der Mandant sie mit dieser E-Mail-Adresse bestätigt hat.

Quelle: Der Artikel wurde uns vom Präsidenten der Steuerberaterkammer Düsseldorf, Herrn Reinhard Verholen, Stb, freundlicherweise zur Verfügung gestellt.

Keine Berichtigung bei Übernahme elektronisch übermittelter Lohndaten anstelle des vom Arbeitnehmer erklärten Arbeitslohns

keyboard_arrow_down

Pressemitteilung Nr. 14 vom 14. März 2018 (Bundesfinanzhof)

Umsatzsteuerrechtliche Gleichbehandlung von Pharmarabatten

keyboard_arrow_down

Pressemitteilung Nr. 17 vom 21. März 2018 (Bundesfinanzhof)

DEUTSCHER STEUERBERATERKONGRESS, 14./15 Mai 2018, Berlin

keyboard_arrow_down

Zum 56. Mal veranstaltet die BStBK den DEUTSCHEN STEUERBERATERKONGRESS.
Alle Informationen finden Sie **hier**.

9. Internationaler Deutscher Steuerberaterkongress, 04./05. Oktober 2018, Amsterdam

keyboard_arrow_down

Deutschsprachige Referenten aus den Bereichen Rechts- und Steuerberatung, die überwiegend in den Niederlanden arbeiten, erläutern den Teilnehmern alles Wissenswerte zu den aktuellen steuerlichen und rechtlichen Rahmenbedingungen der Niederlande.

Weitere Infos finden Sie **hier**.

Veranstaltungshinweise

Hier finden Sie aktuelle Termine und Veranstaltungen.

Unsere aktuellen Pressemitteilungen finden Sie wie immer **hier**.