

Mitteilung der Bundessteuerberaterkammer

6. März 2018

Datenschutz-Grundverordnung der EU (DSGVO)
Handlungsempfehlung für Steuerberaterkanzleien

Ab dem Stichtag 25. Mai 2018 wird die Datenschutz-Grundverordnung (DSGVO) und das neu gefasste BDSG-2018 unmittelbar zu beachten sein. Mit den folgenden Umsetzungsmaßnahmen können sich die Kanzleien schrittweise auf die neuen Anforderungen einstellen:

1. An erster Stelle steht die Einrichtung eines **Datenschutz-Leitfadens**, der für die Kanzleiangehörigen verbindlich ist. Damit wird die „Rechenschaftspflicht“ zur Umsetzung der folgenden Datenschutzgrundsätze dokumentiert: Rechtmäßigkeit, faire Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Richtigkeit sowie technische und organisatorische Maßnahmen (TOM) zum Schutz vor unbefugten Zugriffen oder Beschädigung der personenbezogenen Daten („Integrität und Vertraulichkeit“).
2. Kanzleien kommen nicht umhin, ein **Verarbeitungsverzeichnis** zu erstellen, schon weil in der Steuerkanzlei sensible Daten im Sinne von Art. 9 DSGVO verarbeitet werden. Im Verarbeitungsverzeichnis werden die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung und die Kategorien der Betroffenen, der erhobenen Daten sowie der Empfänger dokumentiert. Zudem müssen die Fristen zur Löschung der in der Kanzlei erhobenen personenbezogenen Daten festgelegt werden. Im Falle einer Datenübertragung in ein Drittland außerhalb der EU/des EWR muss auch dies im Verfahrensverzeichnis geregelt sein (ggf. in Fällen der Nutzung von Cloud-Software, Messenger-Diensten mit Servern in Drittländern etc.).
3. Es empfiehlt sich die Erstellung eines **Aufbewahrungs- und Löschkonzepts**, welches die Einhaltung der Aufbewahrungsfristen und die anschließende Löschung personenbezogener Daten regelt. Auf diese Weise wird die Einhaltung der Löschpflichten dokumentiert.
4. Um die unverzügliche Benachrichtigung der Datenschutzbehörde und Betroffenen (spätestens innerhalb von 72 Stunden) sicherzustellen, eignet sich die Errichtung eines **Meldesystems für Datenpannen**.
5. Die Kanzlei sollte zudem eine Arbeitsanweisung zur Wahrung der **Betroffenenrechte** erstellen: Anhand der Arbeitsanweisung muss das Kanzleipersonal vorbereitet sein, Ansprüche von Betroffenen auf Information und Auskunft, Berichtigung, Löschung und Übertragung von Daten richtig einzuschätzen. Das Kanzleipersonal muss insbesondere bei Drittbetroffenen geltend gemachte Ansprüche ggf. ablehnen, wenn das Berufsgeheimnis des Steuerberaters und seiner Berufsangehörigen Vorrang hat.



6. Kanzleien müssen prüfen, ob ein **Datenschutzbeauftragter (DSB)** bestellt werden muss und ggf. eine **Datenschutz-Folgenabschätzung (DSFA)** durchzuführen ist. Sind zehn oder mehr Personen in der Kanzlei ständig mit der automatisierten Verarbeitung von personenbezogenen Daten befasst, muss immer ein DSB bestellt werden. Ein DSB und eine DSFA ist zudem auch bei weniger als zehn Personen erforderlich, wenn eine besonders umfangreiche Verarbeitung „sensibler“ Datenkategorien (z. B. Daten über die Religion, Gesundheit, sexuelle Orientierung etc.) oder von personenbezogenen Daten über Straftaten vorliegt. Der Begriff einer „besonders umfangreichen Verarbeitung“ ist momentan noch mit Rechtsunsicherheit verbunden.
7. Die **Auftrags(daten)verarbeitungsverträge** (z. B. Kanzleisoftware) müssen an die DSGVO und an die Neufassung der Vorschriften über das Berufsgeheimnis (§ 62a StBerG, § 203 StGB) angepasst werden. Bei Auftragsverarbeitern wie auch bei sonstigen Dienstleistern, die mit personenbezogenen Daten in Berührung kommen, müssen die erforderlichen Erklärungen zur Verschwiegenheit dokumentiert sein. Es muss darauf geachtet werden, dass Auftragsverarbeiter und andere Dienstleister nicht mehr als erforderlich Einblick in die personenbezogenen Daten bekommen. Die Tätigkeit des Steuerberaters nach dem StBerG für seinen Mandanten erfolgt in eigener Verantwortung und ist keine Auftragsverarbeitung. Dies gilt auch für die Lohn- und Gehaltsabrechnung, die der Steuerberater nach dem StBerG eigenverantwortlich ausführt.¹
8. Eine auf die Bedürfnisse der Kanzlei abgestimmte **Schulungsunterlage** dient der Sensibilisierung der Mitarbeiter und Berufsträger. Die Angehörigen der Steuerkanzlei müssen die Grundsätze und Pflichten einer datenschutzkonformen Verarbeitung nach den neuen Vorschriften in der Praxis umsetzen. Die Kanzleiangehörigen müssen in die Lage versetzt werden, bei Anfragen von Betroffenen und Datenschutzbehörden richtig zu reagieren und dabei das Berufsgeheimnis zu wahren.

Zur Umsetzung der vorstehenden Handlungsmaßnahmen bieten die einschlägigen Fachverlage und Datenschutz-Institutionen bereits die ersten Merkblätter und Musterformulare an. Derzeit erarbeiten BStBK und DStV umfassende Praxishilfen, die auf die Anforderungen der kleinen und mittelständischen Steuerberatungskanzleien abgestimmt werden.

¹ DSK-Kurzpapier Nr. 13 „Auftragsverarbeitung“, veröffentlicht z. B. unter:
https://www.lida.bayern.de/de/datenschutz_eu.html, <https://www.lidi.nrw.de>