Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

DEUTSCHER STEUERBERATER-VERBAND e.V.

Antworten auf häufig gestellte Fragen zur Datenschutz-Grundverordnung (DSGVO)

Stand: 4. April 2018

Zum 25. Mai 2018 müssen die neuen Vorschriften der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG 2018) umgesetzt werden. In diesem Zusammenhang sind im Berufsstand vermehrt Fragen zur neuen DSGVO entstanden. Die Bundessteuerberaterkammer (BStBK) und der Deutsche Steuerberaterverband e.V. (DStV) geben nachfolgend gemeinsam Antworten auf die am häufigsten gestellten Fragen. Sie sollen als Checkliste zur zielgerichteten Vorbereitung auf das neue Datenschutzrecht dienen und erheben keinen Anspruch auf Vollständigkeit. Einige Fragen sind aufgrund der unbestimmten Rechtsbegriffe und der nicht vorhandenen Behördenpraxis und Rechtsprechung zu den neuen Vorschriften derzeit noch nicht abschließend geklärt. Auch steht in manchen Bereichen eine abgestimmte Meinungsbildung der Aufsichtsbehörden für den Datenschutz noch aus.

Die nachfolgenden Antworten geben daher nur die gemeinsame, abgestimmte Meinung der BStBK und des DStV zum Zeitpunkt der Veröffentlichung wieder. Eine Rechtsberatung im Einzelfall kann dadurch nicht ersetzt werden. Vielmehr sollten rechtliche Fragen mit Blick auf die konkrete Umsetzung des Datenschutzes in der jeweiligen Steuerberatungskanzlei stets gesondert geprüft werden. Für Aktualität, Richtigkeit und Vollständigkeit der in diesem FAQ-Katalog enthaltenen Antworten kann keine Haftung übernommen werden. Insbesondere müssen die Entwicklungen von Behördenpraxis und Rechtsprechung durch die Kanzleien weiter beobachtet werden.

BStBK und DStV werden weitere Umsetzungshilfen für die Praxis veröffentlichen.

Inhaltsverzeichnis

1. Welche Verarbeitungstätigkeiten gibt es in einer Steuerberatungskanzlei?

Eine abschließende Aufzählung der Verarbeitungstätigkeiten ist nicht möglich. Diese müssen vielmehr anhand der tatsächlichen Tätigkeiten in der Kanzlei im Einzelfall konkret bestimmt werden. Eine Übersicht über die wesentlichen Verarbeitungstätigkeiten ergibt sich aus der Aufstellung „Anforderungen für Steuerberater" des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA). Diese sind z. B.:

- Lohn- und Gehaltsabrechnung der Mitarbeiter
- Verarbeitung von Mandantendaten von Privatkunden zur Beratung und Rechnungsstellung
- Verarbeitung von Mandantendaten von Firmenkunden und deren Kunden/Mitarbeitern zur Beratung und Rechnungsstellung
- Betrieb der Webseite über Dienstleister

Siehe: https://www.lda.bayern.de/de/kleine-unternehmen.html

2. Gibt es eine Übersicht der Verfahren, die der Steuerberater im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO zu beschreiben hat?

Die Kanzleien können sich an ihrem bisherigen Verfahrensverzeichnis orientieren. Ein für Steuerberater spezifisches Muster von der BStBK und dem DStV ist hier abrufbar:

https://www.bstbk.de/de/presse/news/2018-04-05_Praxishilfen_Datenschutz/index.html

Die Datenschutzkonferenz hat ebenfalls Templates für die Verzeichnisse der Verarbeitungstätigkeiten veröffentlicht, an denen man sich orientieren kann:

https://www.lda.bayern.de/de/kleine-unternehmen.html

3. Sind Erleichterungen für kleinere Kanzleien vorgesehen?

Nein, die Vorgaben der DSGVO gelten grundsätzlich unabhängig von der Größe des Unternehmens.

4. Welches sind die wichtigsten Umsetzungsschritte, die jetzt in der Praxis zu beachten sind?

Die BStBK und der DStV haben eine Übersicht über die wichtigsten Umsetzungsmaßnahmen für Steuerberatungskanzleien veröffentlicht:

Fachinfo der BStBK: „Handlungsempfehlung für Steuerberaterkanzleien zur Datenschutz-Grundverordnung (DSGVO)“, abrufbar unter https://www.bstbk.de/de/presse/publikationen/

DStV-Information: „EU-Datenschutzgrundverordnung (DSGVO) – Handlungsempfehlungen für Steuerberatungskanzleien“, abrufbar unter https://www.dstv.de/interessenvertretung/beruf/beruf-aktuell/tb-58-18-cm-dsgvo

5. Ist eine Personalnummer ein personenbezogenes Datum?

Eine Personalnummer ist ein personenbezogenes Datum, weil diese Information einer natürlichen Person zugeordnet werden kann.

6. Wer darf zum Datenschutzbeauftragten (DSB) bestellt werden?

DSB kann jeder Mitarbeiter oder externer Dienstleister sein, der über entsprechende Kenntnisse verfügt. Ausgeschlossen sind jedoch die Mitglieder der Kanzleileitung (Verantwortliche), Beschäftigte in leitender Funktion und der EDV-Administrator bzw. EDV-Betreuer.

7. Wie erfolgt die Berechnung der Mitarbeiteranzahl für den DSB? Zählt die Anzahl der Köpfe? Zählen die Teilzeitkräfte anders bei der Berechnung? Werden die Beschäftigten in einer Bürogemeinschaft zusammengezählt?

Die Voraussetzungen richten sich an der Personenanzahl aus, unabhängig von deren arbeitsrechtlichem Status oder deren Arbeitszeit. Daher sind auch Auszubildende, Praktikanten, freie Mitarbeiter, Teilzeitkräfte oder Rechtsreferendare voll mitzuzählen. Derzeit ist noch nicht abschließend geklärt, ob der/die Kanzleiinhaber mitzurechnen ist/sind.

Bei Bürogemeinschaften ist ein Zugriff auf die Daten des anderen Bürogemeinschaftspartners nicht zulässig (Datentrennung). Daher werden nur Personen, die für alle Beteiligten tätig sind (bspw. in einem Sekretariat für zwei Berufsträger) bei der Berechnung aller Beteiligten berücksichtigt.

8. Welche datenschutzrechtlichen Vorgaben müssen bei der Kanzlei-Webseite beachtet werden?

Die Anforderungen bei der Verarbeitung personenbezogener Daten richten sich zusätzlich nach dem Telemediengesetz (TMG). Bei der Verwendung von Formularfeldern

oder Logins zu geschlossenen Benutzerbereichen wird eine Seitenverschlüsselung als erforderlich angesehen. Im Übrigen finden weitere Abstimmungen im Rahmen der Datenschutzkonferenz des Bundes und der Länder (DSK) statt. Die BStBK und der DStV beobachten die Entwicklung und werden hierzu berichten.

9. Gibt es eine Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist?

Die Aufsichtsbehörden werden eine Liste von Verarbeitungstätigkeiten veröffentlichen, bei denen eine Datenschutz-Folgenabschätzung erforderlich ist (Art. 35 Abs. 4 DSGVO). Darüber hinaus gelten die gesetzlichen Anforderungen aus Art. 35 DSGVO.

Steuerberater benötigen für ihre Kerntätigkeit keine DSFA.

Siehe dazu die Arbeitshilfe des BayLDA „Anforderungen für Steuerberater“:

https://www.lda.bayern.de/de/kleine-unternehmen.html

Die Notwendigkeit zur DSFA könnte sich jedoch ggf. aus einem anderen Kontext (z. B. Videoüberwachung) ergeben und sollte dann entsprechend geprüft werden.

10. Können die Einwilligungserklärungen in den Mandatsvertrag integriert werden?

Die betroffene Person kann nur unter Beachtung bestimmter Formvorschriften einwilligen. Daher ist in der Regel von der Integration der Einwilligung in den Fließtext des Mandatsvertrages abzuraten.

11. Kann der Mandant in den unverschlüsselten Versand von E-Mails mit den Daten seiner Arbeitnehmer einwilligen?

Nein, einwilligen kann nur eine betroffene Person.

12. Müssen auch E-Mails z. B. an Lieferanten verschlüsselt werden?

Bei Übermittlung personenbezogener Daten sind angemessene Schutzmaßnahmen zu prüfen.

13. Liegt eine Auftragsverarbeitung vor, wenn die Mandanten mit einer Unterberaternummer auf dem System des Steuerberaters selbst buchen?

Berufsrechtlich ist die Überlassung von Software und die Verschaffung der Möglichkeit, die Daten direkt in dem EDV-System des Beraters zu erfassen, nur im Rahmen eines bestehenden Auftrags- und Mandatsverhältnisses zulässig. Daher erfolgt die Verschaffung dieser Möglichkeiten im Rahmen der Tätigkeiten des Steuerberaters für seinen Mandanten. Diese Tätigkeiten stellen – auch nach Auffassung der Datenschutzkonferenz (Kurzpapier Nr. 13 vom 16. Januar 2018, Anhang B) – keine Auftragsverarbeitung dar. Siehe hierzu ebenfalls:

> Fachinfo der BStBK: „Handlungsempfehlung für Steuerberaterkanzleien zur Datenschutz-Grundverordnung (DSGVO)“:
> https://www.bstbk.de/de/presse/publikationen/
>
> DStV-Information: „EU-Datenschutzgrundverordnung (DSGVO) – Handlungsempfehlungen für Steuerberatungskanzleien“:
> https://www.dstv.de/interessenvertretung/beruf/beruf-aktuell/tb-58-18-cm-dsgvo

14. Handelt es sich beim Führen der Vollmachtsdatenbank um eine Auftragsverarbeitung?

Die Vollmachtsdatenbank wird nicht durch die Steuerberaterkammern selbst geführt. Vielmehr hat die BStBK einen Rahmenvertrag mit der DATEV eG abgeschlossen. Auf Basis des Rahmenvertrages ist abgestimmt, dass den Kammermitgliedern eine Vereinbarung zur Auftragsverarbeitung angeboten wird. Mittels Dienstleistungen der DATEV eG kann auf die Daten der Finanzverwaltung zugegriffen werden. Dafür ist zwischen der Steuerberatungskanzlei und der DATEV eG eine Vereinbarung zur Auftragsverarbeitung abzuschließen.

15. Kann der DATEV-Vertrag zur Auftragsverarbeitung ohne Bedenken unterschrieben werden?

Der Vertrag ist laut Information der DATEV eG mit dem BayLDA abgestimmt. Bei Bedenken wegen einzelner Passagen sollte man sich mit der DATEV eG in Verbindung setzen.

16. Wird die Einschätzung der deutschen Datenschutzkonferenz bzgl. des Nichtvorliegens einer Auftragsverarbeitung bei Einschaltung eines Steuerberaters auch von anderen europäischen Aufsichtsbehörden geteilt?

Grundsätzlich ist jede Aufsichtsbehörde in ihrer rechtlichen Beurteilung unabhängig. Die Einschätzungen der ausländischen Aufsichtsbehörden sind der BStBK und dem DStV nicht bekannt.

17. Müssen im Rahmen der Erfüllung des Auskunftsanspruchs auch dann Kopien zur Verfügung gestellt werden, wenn der Mandant im Laufe des Mandatsverhältnisses bereits Kopien erhalten hat?

Grundsätzlich ja, denn der Auskunftsanspruch muss die natürliche Person in die Lage versetzten zu überprüfen, ob die Verarbeitung der aktuellen Daten noch den Anforderungen an die Rechtmäßigkeit und Zweckbindung genügen.

18. Unterliegt der Auskunftsanspruch nach Art. 15 DSGVO der Verjährung?

Ein Auskunftsanspruch nach Art. 15 DSGVO kann immer nur aktuell gestellt werden, d. h. immer nur für die Daten, die zum Zeitpunkt der Auskunftserteilung noch vorhanden sind. Verstöße gegen die Auskunftspflicht unterliegen der Verjährung nach dem Gesetz über Ordnungswidrigkeiten (OWiG).

19. Wie werden die Löschfristen bestimmt?

Die Löschfristen bestimmen sich nach den gesetzlichen Aufbewahrungspflichten. Der Steuerberater hat in vielen Fällen die Verpflichtung zur Aufbewahrung im Rahmen des Mandatsverhältnisses übernommen.

Der Umfang der aufbewahrungspflichtigen Unterlagen wird auch von der Finanzverwaltung nicht abschließend bestimmt. Sowohl Gesetzgebung (z. B. KassenSichV) und Rechtsprechung, als auch Finanzverwaltung (z. B. in den GoBD) erweitern eher den Bereich der Aufbewahrungspflichten und deren Dauer. Im Rahmen des Löschkonzeptes ist daher zu prüfen, ob Rechtfertigungsgründe für eine Verlängerung des Aufbewahrungszeitraums vorliegen.

20. Kann ein Mandant seine Einwilligung darin erteilen, dass seine Daten nie gelöscht werden?

Eine solche Einwilligung ist theoretisch möglich. Da die im Rahmen eines Mandates gespeicherten Daten aber häufig auch schutzwürdige Daten anderer Personen beinhalten, müsste der Mandant zur Erteilung einer solchen Erlaubnis die Zustimmung dieser Drittbetroffenen einholen.

Empfehlenswert ist es daher, nach Ablauf der gesetzlichen Aufbewahrungspflichten und vor Löschung der Daten ggf. gemeinsam mit dem Mandanten zu prüfen, ob besondere Rechtfertigungsgründe (z. B. Verschlechterung der Rechtsposition gegenüber den Finanzbehörden u. ä.) für eine längere Aufbewahrung vorliegen.

21. Wie gehen die Finanzbehörden mit den Löschanforderungen um? Müssen die Behörden auch löschen?

Die DSGVO gilt für öffentliche Stellen (Behörden) und Unternehmen gleichermaßen. Ergänzend gelten die Regelungen des BDSG 2018 und der Abgabenordnung, die für öffentliche Stellen bzw. Finanzbehörden Sonderregelungen vorsehen.

Muster

Verzeichnis von Verarbeitungstätigkeiten der Steuerberatungskanzlei im Sinne von Art. 30 Datenschutz-Grundverordnung (DSGVO) (Stand: tt.mm.jjjj)

Verantwortlicher	
Name der verantwortlichen natürlichen oder juristischen Person	
Ansprechpartner, ggf. gesetzlicher Vertreter	
Postadresse	
Telefon	
E-Mail-Adresse	

Datenschutzbeauftragter	
Nachname, Vorname	
Postadresse	
Telefon	
E-Mail-Adresse	

Verarbeitungstätigkeit lfd. Nr. 1: Personalverwaltung	
Zwecke der Verarbeitung	Verwaltung der Personalangelegenheiten Einstellung von Personal Abwicklung von Arbeitsverträgen
Kategorien betroffener Personen	Beschäftigte
Kategorien von personenbezogenen Daten	Stammdaten Arbeitsunfähigkeitsbescheinigungen Schriftverkehr Bewerbungsunterlagen Leistungsbeurteilungen Zeitaufzeichnungen
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	Personalabteilung Rechnungswesen Sozialversicherungsträger Finanzbehörden Kreditinstitute Versicherungen Gerichte Gläubiger
Ggf. Datenübermittlung in Drittstaaten	keine

Fristen für die Löschung der Datenkategorien	Siehe Löschkonzept
Technische und organisatorische Maßnahmen	Siehe IT-Sicherheitskonzept

Verarbeitungstätigkeit lfd. Nr. 2: Finanzbuchhaltung (siehe Prozess im QM-/QS-Handbuch)	
Zwecke der Verarbeitung	Erstellen von Finanzbuchhaltung, Nebenbüchern sowie Übermittlung an Behörden und andere Stellen
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten Debitoren von Mandanten Kreditoren von Mandanten Beschäftigte der Behörden Kooperationspartner und deren Beschäftigte Beschäftigte von Versicherungen
Datenkategorien	Stammdaten des Mandanten Bewegungsdaten im Rahmen der Finanzbuchhaltung Schriftverkehr
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	Behörden Mandanten Sonstige Dritte auf Wunsch der Mandanten
Ggf. Datenübermittlung in Drittstaaten	Grundsätzlich keine; in Sonderfällen im (zusätzlichen) Auftrag des Mandanten
Fristen für die Löschung der Datenkategorien	Siehe Löschkonzept
Technische und organisatorische Maßnahmen	Siehe IT-Sicherheitskonzept

Weitere Verarbeitungstätigkeiten ergänzen:

Verarbeitungstätigkeit lfd. Nr. ……:	
Zwecke der Verarbeitung	
Kategorien betroffener Personen	
Datenkategorien	
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	

Ggf. Datenübermittlung in Drittstaaten	
Fristen für die Löschung der Datenkategorien	
Technische und organisatorische Maßnahmen	

Im IT-Sicherheitskonzept sollte zumindest auf folgende Aspekte eingegangen werden:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
    - Zutrittskontrolle
    - Zugangskontrolle
    - Zugriffskontrolle
    - Trennungskontrolle
    - Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) in Ausnahmefällen

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)
    - Weitergabekontrolle
    - Eingabekontrolle

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
    - Verfügbarkeitskontrolle
    - Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
    - Datenschutz-Management
    - Incident-Response-Management
    - Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
    - Auftragskontrolle

Muster für ein Löschkonzept

Die Einhaltung der Löschfristen wird durch die Kanzleileitung oder eine durch diese beauftragte Person einmal jährlich überprüft. Das Ergebnis dieser Überprüfung ist zu dokumentieren.

Übersicht über die Löschfristen:

	XX	**6 Monate**	**10 Jahre**	**14 Jahre**		
Beschäftigtendaten			Nach Ausscheiden			
Finanzbuchhaltung				Prüfen		
…						
…						